DR_POLÍTICA DE SEGURIDAD Y GESTIÓN DE LA INFORMACIÓN	
Macro-Proceso	Gestión de Relaciones con el Cliente.

Elaborado Por	Revisado Por	Aprobado Por
Jesús Guzmán Coordinador de Gestión Tecnológica	Valentina Cadavid Gerente de Operaciones	Fabio Pineda Callejas Gerente General
Fecha 2020/07/27	**Fecha** 2020/07/30	**Fecha** 2020/08/06

CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
2020/04/30	01	Creación del documento.
2020/08/06	02	Actualización documento, se incluyen los lineamientos para: manejo de dispositivos móviles, borrado seguro y destrucción de la información, transferencia e intercambio de información, estándares de control de acceso lógico a plataformas tecnológicas, manejo de pantalla y escritorio limpio, registros de auditoría de logs y su supervisión, gestión de la vulnerabilidad técnica y desarrollo de software seguro.

1. Objetivo.

Establecer los lineamientos necesarios para proteger, preservar y administrar correctamente la información de **PERSONALSOFT**, junto con las tecnologías utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

Crear una la Política de Seguridad de la Información que esté basada y sirva como marco de referencia a la futura implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma IS027001 para Personalsoft.

2. Alcance.

Esta política aplica a todas las áreas que componen la organización, a sus recursos, a la totalidad de los procesos internos o externos vinculados a Personalsoft a través de contratos o acuerdos con terceros y a todo el personal de Personalsoft, cualquier sea su situación contractual, la dependencia a la cual fue contratado y el nivel de las tareas o funciones que desempeñe.

3. Glosario.

- **Activos:** cualquier componente (humano, tecnológico, software, manuales, documentación, entre otros) que tiene valor para la organización y signifique riesgo si llega a manos de personas no autorizadas.

- **Antivirus:** El antivirus es un programa que ayuda a proteger su computadora contra la mayoría de los virus, troyanos y otros invasores indeseados que puedan infectar su ordenador o equipo.

- **Aplicación:** programa informático diseñado para permitir a los usuarios la realización de tareas específicas en computadores, servidores y similares.

- **Base de datos:** conjunto de datos almacenados y organizados con el fin de facilitar su acceso y recuperación.

- **Backups o copias de respaldo:** copia que se realiza a la información institucional definida como sensible o vulnerable, con el fin de utilizarla posteriormente para restablecer el original ante una eventual pérdida de datos, para continuar con las actividades rutinarias y evitar pérdida generalizada de datos

- **Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- **Código fuente:** conjunto de instrucciones escritas en algún lenguaje de programación de computadoras, hechas para ser leídas y transformadas por alguna herramienta de software (compilador, intérprete, ensamblador) en lenguaje de máquina o instrucciones ejecutables en el computador.

- **Credenciales de acceso:** privilegios de seguridad agrupados bajo un nombre y contraseña, que permiten acceso a los sistemas de información.

- **Datacenter, centro de datos o sala de servidores**: área dispuesta para el alojamiento seguro de los equipos de cómputo necesarios para el procesamiento y almacenamiento de la información de una organización (Servidores, SAN, equipos de comunicación, etc.).

- **Disponibilidad:** propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

- **Dispositivo móvil:** Aparato electrónico con capacidades de cómputo y conexión a redes inalámbricas cuyo tamaño y diseño permite ser fácilmente transportado para utilizarse en diversas ubicaciones con facilidad (portátiles, tablets, celulares inteligentes y demás dispositivos con características similares).

- **Integridad:** propiedad de salvaguardar la exactitud y el estado completo de los activos.

- **Impacto:** la consecuencia que al interior de la empresa se produce al materializarse una amenaza.

- **Evento de seguridad de la información:** presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

- **Medios Removibles:** Los dispositivos de almacenamiento removibles son dispositivos de almacenamiento independientes del computador y que pueden ser transportados libremente.

- **Propietario:** En la estructura administrativa de la organización, se le otorga la propiedad del activo a cada una de las unidades estratégicas, divisiones organizacionales, gerencias y direcciones.

- **Seguridad de la Información:** Preservación de la confidencialidad, disponibilidad e integridad de la información (ISO/IEC 27000) independiente de su medio de conservación, transmisión o formato.

- **Servidor:** Equipo de computación físico o virtual, en el cual funciona un software, cuyo propósito es proveer servicios a otros dispositivos dentro de la red.

- **Servidor de almacenamiento o file server:** equipo servidor dotado con varios discos duros destinados a respaldar y compartir datos.

- **Riesgo:** combinación de la probabilidad de un evento y sus consecuencias.

- **TI:** Se refiere a tecnologías de la información.

- **TIC:** Se refiere a tecnologías de la información y comunicaciones.

- **VPN:** Una VPN (Virtual Private Network) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar estas redes para que sus empleados, desde sus casas, hoteles, etc., puedan acceder a recursos corporativos que, de otro modo, no podrían.

- **VSTS (Visual Studio Team Services):** es un sistema de gestión del ciclo de vida de la aplicación que ayuda a todo el equipo del proyecto a capturar requisitos, planificación de proyectos ágil / tradicional, gestión de elementos de trabajo, control de versiones, compilación, implementación y pruebas manuales, todo en una sola plataforma.

- **Vulnerabilidad:** debilidad de un activo o grupo de activos, que puede ser aprovechada por una o más amenazas.

4. Descripción de las Políticas.

4.1. Cumplimiento.

El cumplimiento de la Política de Seguridad y Gestión de la Información es obligatorio. Si los colaboradores, proveedores, terceras partes violan estas políticas, la organización se reserva el derecho de tomar las medidas correspondientes.

4.2. Excepciones.

Las excepciones a cualquier cumplimiento de la Política de Seguridad y Gestión de la Información deben ser aprobadas por la Gerencia General, la cual puede requerir autorización de la Gerencia de Operaciones, Gerencia Financiera, Gerencia Comercial y del Comité corporativo. Todas las excepciones a la Política deben ser formalmente documentadas, registradas y revisadas.

4.3. Administración de las políticas.

Las modificaciones o adiciones de la Política de Seguridad y Gestión de la Información serán propuestas por la Gerencia de Operaciones, la Gerencia Administrativa y Financiera, la Gerencia Comercial, por medio de la Gerencia General y serán aprobadas por el Comité. Estas políticas deben ser revisadas como mínimo una vez al año o cuando sea necesario.

5. Dispositivos móviles.

Se permite el uso de dispositivos móviles de conexión inalámbrica al interior de las instalaciones de Personalsoft, únicamente para desarrollar y cumplir con los objetivos laborales y/o contractuales del personal, procurando no almacenar en estos dispositivos información organizacional y siempre en cumplimiento de la política de red inalámbrica (DR_PolíticaRedInalámbrica) publicada en el Portal SIG.

Los dispositivos móviles asignados a nuestros colaboradores, son de propiedad de PersonalSoft y los responsables de dichos equipos, deberán velar por su adecuado uso, cuidado, mantenimiento y protección.

Los medios de almacenamiento de estos dispositivos serán protegidos tecnológicamente con medios de cifrado de datos o mediante cualquier otro mecanismo definido por el área de Gestión Tecnológica, con el fin de evitar la interceptación y/o uso indebido de la información que en ellos se almacene.

La solicitud de conexión de dichos dispositivos a la red inalámbrica de la organización se debe realizar a través de un requerimiento generado por el jefe inmediato en la herramienta GLPI.

Se prohíbe el ingreso de teléfono celulares y otros dispositivos móviles a los centros de datos y centros de cableado de PersonalSoft, salvo que exista una autorización explícita emitida por el área de Gestión Tecnológica.

La alta dirección de la organización podrá exigir para determinadas reuniones la ausencia de dispositivos móviles, dispositivos de grabación y cualquier otro equipo electrónico que se especifique por razones confidencialidad o de evitar la interceptación y/o uso indebido de la información que en ellos se almacene.

Para los visitantes y personal de apoyo que ingrese a la organización y que requiera para sus funciones o servicios a prestar, el uso de alguno de estos dispositivos móviles, deben aplicarse las mismas restricciones de uso; adicionalmente, deberá estar siempre acompañado del responsable por parte de PersonalSoft para esta visita, con el fin de evitar usos indebidos de las tecnologías.

6. Navegación internet.

El uso de Internet debe estar destinado exclusivamente a la ejecución de las actividades asignadas por PersonalSoft y deben ser utilizados por el colaborador para realizar las funciones establecidas para su cargo; por tal motivo, se crea y publica en el Portal SIG la política de Navegación Internet (SAFdr05_PoliticaNavegaciónInternet) con el objetivo de brindar a los usuarios buenas prácticas para su utilización.

6.1. Red LAN (alámbrica).

Será considerado como un ataque a la seguridad y una falta grave, cualquier actividad no autorizada por el área de Gestión Tecnológica, en la cual los usuarios realicen la exploración de los recursos informáticos en la red de la institución, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

Por este motivo Gestión Tecnológica como responsables de las redes de datos y los recursos de red de Personalsoft, debe velar porque dichas redes sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico el cual se mencionan a continuación:

El usuario debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar un reacomodo de cables con el personal de Gestión Tecnológica.

Todos los cambios en los servidores y equipos de red de Personalsoft, incluyendo la instalación del nuevo software, el cambio de direcciones IP, la reconfiguración de Routers y Switches, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios

apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

La solicitud para la conexión de nuevos equipos a la red de la organización deber hacerse a través del GPI, y desde un correo institucional, por ningún motivo se permitirá la conexión de nuevos equipos sin la previa autorización del área de Gestión Tecnológica.

6.2. Red WIFI (inalámbrica).

Se cuenta con unos controles para uso de la red inalámbrica por los colaboradores y/o terceros para realizar las funciones establecidas para su cargo o tareas asignadas; por tal motivo, se crea y publica en el Portal SIG la política de Red Inalámbrica (DR_Red_Inalambrica) con el objetivo de brindar a los usuarios buenas prácticas para conexión a la red.

7. Activos fijos y recursos de información.

7.1. Activos fijos.

Personalsoft pone al servicio de los colaboradores, el uso de los medios necesarios para el normal desarrollo de las labores propias de sus respectivos cargos; por lo cual adopta y comunica las políticas de uso aceptable, controles y medidas dirigidas a garantizar la seguridad y continuidad del servicio que presta.

Por lo anterior, todos los colaboradores, proveedores o terceras partes, que usen activos de información que sean propiedad de Personalsoft, son responsables de cumplir y acoger con integridad nuestra política de Activos Fijos (SAFdr03_Política Activos Fijos), la cual puede se ser consultada en el Portal SIG.

7.2. Uso del correo electrónico.

Personalsoft, como muestra del respeto por los principios de libertad de expresión y privacidad de información, no genera a los colaboradores ninguna expectativa de privacidad en cualquier elemento que almacene, envíe o que reciba por medio del sistema de correo electrónico propiedad de la compañía; en consecuencia, podrá denegar el acceso a los servicios de correo electrónico, inspeccionar, monitorear y/o cancelar un buzón de correo asignado.

A los colaboradores que de acuerdo con sus funciones requieran una cuenta de correo, esta se les asigna en el servidor una vez son vinculados. Para su asignación, el área de Gestión Humana, es responsable de informar al área de Gestión Tecnológica, las vinculaciones de los colaboradores para la creación de cuenta de correo electrónico; de igual manera debe informar oportunamente los retiros de colaboradores para la suspensión de este servicio.

La cuenta de correo estará activa durante el tiempo que dure la vinculación del colaborador con PersonalSoft; excepto en casos de fuerza mayor o mala utilización, que eventualmente puedan causar la suspensión o cancelación de la misma.

Una vez se produzca la desvinculación del colaborador; el área de Gestión Humana notifica por medio del GLPI la novedad al área de Gestión Tecnológica, así la cuenta de correo electrónico será dada de baja en el servidor.

El correo electrónico es personal e intransferible y le corresponde al colaborador velar por la seguridad de la información protegiendo su clave de acceso, por ende, el usuario es el único responsable su buen uso. En consecuencia, al aceptar el buzón otorgado por PersonalSoft, el usuario se compromete a:

- Respetar la privacidad de las cuentas de otros usuarios del servicio, tanto dentro como fuera de la red corporativa. El usuario no podrá utilizar identidades ficticias o pertenecientes a otros usuarios para el envío de mensajes.

- El uso del correo electrónico propiedad de PersonalSoft y deberá ser usado solamente para fines propios a la organización. En su uso el colaborador actuará siempre con respeto y cortesía; no podrá crear, distribuir o reenviar mensajes que ofendan la dignidad, intimidad y buen nombre de las personas de la organización, o para realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil; de igual forma se prohíbe difundir ideas políticas, religiosas, propagandas entre otros.

- El colaborador titular del correo electrónico o cuenta asignada por la PersonalSoft, usará dicho medio para enviar y recibir mensajes necesarios para el desarrollo de las labores propias de su cargo o de las investigaciones que tenga asignadas. Únicamente, la Gerencia de Negocios y la Gerencia Administrativa y Financiera están autorizadas para el envío de correos masivos. Otras necesidades de comunicación masiva deben ser aprobadas por el área de Gestión Tecnológica y área de Comunicaciones.

- Realizar mantenimiento periódico de su correo, cuando el sistema le haga advertencia de espacio disponible.

- Utilizar la cuenta de correo electrónico corporativa para fines laborales, de investigación y lo estrictamente relacionado con las actividades propias de su trabajo. Los colaboradores deben evitar usar el buzón de correo electrónico para fines comerciales diferentes a los que sean relativos al interés de la empresa.

7.3. Uso de herramientas que comprometen la seguridad.

Es muy importante que los colaboradores no realicen cualquier actividad que intente acceder o violar la seguridad de los activos de información, equipos de conectividad sin permisos del anfitrión, del sistema, o del área de Gestión de Tecnológica.

Actividades que pueden comprometer la seguridad:

- Acceder el sistema o red por medios de engaños al sistema.

- Monitorear datos o tráfico en la red de la organización.

- Sondear, copiar, probar firewalls o herramientas de hacking que integren contra los servicios de información.

- Atentar contra la vulnerabilidad del sistema, servicios o redes de la organización.

- Violar las medidas de seguridad o las rutinas de autenticación del sistema o de la red.

7.4. Recursos compartidos.

El uso de carpetas compartidas en los equipos de cómputo de los colaboradores es una práctica muy útil, pero tiene implícitos algunos riesgos que pueden afectar los principios de confidencialidad, integridad y disponibilidad de la información, por lo tanto, su uso y aplicación debe ser controlado.

Con este propósito la organización define los siguientes lineamientos para su uso seguro:

- Se debe evitar el uso de carpetas compartidas en equipos de escritorio.

- El usuario que autoriza y dispone el recurso compartido es el responsable por las acciones y los accesos sobre la información contenida en dicha carpeta.

- Se debe definir el tipo de acceso y los roles estrictamente necesarios sobre la carpeta (lectura, escritura, modificación y borrado).

- Si se trata de información confidencial o crítica para la empresa, deben utilizarse las carpetas destinadas para tal fin en el servidor de archivos PSDATOS de usuarios, para que sean incluidos en las copias diarias de respaldo de información o implementar herramientas para el respaldo continuo de información.

- El acceso a carpetas compartidas debe delimitarse a los usuarios que las necesitan y deben ser protegidas con contraseñas.

- No se debe permitir el acceso a dichas carpetas a usuarios que no cuenten con antivirus corporativo actualizado.

7.5. Computación en nube.

Ninguna información de Personalsoft podrá utilizar tecnologías de computación en nube si no está previamente autorizado por el área de Gestión de Tecnológica.

7.6. Uso de redes virtuales o conexiones VPN.

El uso de herramienta VPN permite la conexión de manera segura a través de un túnel que hace conexión con la red privada de la organización a continuación se indica el uso de esta.

7.6.1. Conexión VPN Personalsoft.

A continuación, se realiza la descripción de los siguientes escenarios:

- **Equipo de Personalsoft:** Los equipos de Personalsoft al momento de ser entregados ya cuentan con el cliente VPN el cual pueden acceder para su conexión a través de la autenticación del usuario de red previamente asignado por el área de Gestión Tecnológica.

  A cada colaborador que le sea asignado un equipo o recursos por la organización este deberá firmar el Acta Entrega Activos (SAFpl10_ActaEntregaActivosF) donde se compromete a dar un uso adecuado a los recursos asignados.

- **Equipo propio del Colaborador:** El uso de equipos propio del empleado solo aplicará en caso de que el colaborador sea contratado y no tenga asignación de un equipo por Personalsoft debido a que se encuentra fuera de la ciudad.

  El jefe inmediato deberá generar un GLPI indicando la necesidad de la instalación, configuración de la VPN en el equipo propio del colaborador al área de Gestión Tecnológica donde el analista de TI será el encargado de proceder con la configuración e instalación y así mismo capacitará al colaborador para el uso de la herramienta y conexión a los servicios y servidores de Personalsoft dependiendo su rol o cargo.

7.6.2. Conexión VPN clientes.

A continuación, se realiza la descripción de los siguientes escenarios:

- **Equipo Personalsoft:** Para la conexión de VPN de clientes (Personal Especializado), el cliente notificará la política de acceso y el colaborador debe adherirse a las políticas notificadas por el cliente.

  El jefe inmediato deberá generar un GLPI indicando la necesidad de la instalación, configuración de la VPN del cliente en el equipo asignado al colaborador donde el analista de TI del área de Gestión Tecnológica será el encargado de proceder con la instalación y configuración y el cliente deberá capacitar al colaborador sobre el uso de la herramienta.

- **Equipos de Clientes:** Para la conexión de VPN de clientes (Personal Especializado), el cliente será el encargado de realizar la instalación, configuración y capacitación para el uso de la herramienta y notificará la política de acceso o conexión VPN donde el colaborador debe adherirse a las políticas notificadas por el cliente.

- **Equipo Propio del Colaborador:** El uso de equipo propio del empleado solo aplicará en caso de que el colaborador sea contratado y no tenga asignación de un equipo por Personalsoft o del Cliente debido a que se encuentra fuera de la ciudad.

En caso de requerirse esta configuración el jefe inmediato deberá solicitar al cliente a través de un requerimiento la instalación, configuración de las herramientas, aplicaciones que requiera el colaborador para desempeñar sus funciones o tareas asignadas.

En caso de solo requerir conexión de tipo remoto, por parte del cliente no se debe permitir conexión directa a la red del cliente, solo se debe habilitar el tráfico de escritorio

remoto y se debe bloquear la navegación desde el equipo personal mientras esté conectado a la VPN.

7.7. Tipo y clasificación de la información.

La información se clasifica en tres grupos; publica, uso interno y confidencial. Esta clasificación, para la información que se encuentre en los servidores, estará en el Inventario de activos. Para la información que se encuentre fuera de los servidores, independiente del medio, la clasificación deberá incluirse en el documento como marca de agua. Las siguientes son las directrices para clasificación:

7.7.1. Información No crítica.

Información que está disponible para personal interno y externo incluyendo empleados, clientes y público en general. Sin restricciones de acceso. Incluye:

- **Pública:** Información disponible en páginas como formularios Google (Sites), (Sharepoint) o portal empresarial www.personalsoft.com.

- **Uso interno:** información en intranet, sistema documental, procedimientos del sistema de gestión y aplicaciones que soportan Backoffice de la compañía.

7.7.2. Información crítica.

La información es CONFIDENCIAL y está disponible solo para personal autorizado mediante el control de acceso restringido, autenticación vía web, servicios de directorio, LDAP.

8. Contraseñas y control de acceso a la información.

8.1. Gestión control acceso.

Es responsabilidad de área de talento humano, informar al área de Gestión Tecnológica sobre los nuevos colaboradores que ingresan a la organización, con el fin de poder asignar los respectivos permisos para el acceso a los recursos tecnológicos de la organización.

Gestión Tecnológica es el área encargada de definir y suministrar los mecanismos de acceso lógico para la asignación de permisos y privilegios a los usuarios de acuerdo a sus

funciones, términos contractuales y/o roles definidos al interior de la organización, así como la modificación los permisos y privilegios de los usuarios en los mecanismos y/o sistemas de autenticación definidos.

El área de talento humano es la encargada de notificar y dar los lineamientos para la creación y supresión de usuarios que son contratados por la organización.

Es responsabilidad de área de talento humano, informar o notificar al área de Gestión Tecnológica sobre las finalizaciones de contratos de colaboradores que se retiran de la organización, con el fin de deshabilitar los respectivos permisos de acceso a los recursos tecnológicos de la organización con el que contaba el colaborador.

Los jefes inmediatos de cada colaborador, responsables de los activos de información deben informar inmediatamente sobre las novedades de los derechos de acceso lógico de los usuarios.

Se prohíbe el uso de las cuentas de usuario administrador local en la organización, salvo en aquellos casos que estén debidamente justificados y autorizados.

Los jefes inmediatos, responsables de los activos de información de la organización deben revisar periódicamente los derechos de acceso de los usuarios o de sus colaboradores que son compartidos por el reporte de Tecnología.

Para la creación y administración de las credenciales de acceso organizacional, los colaboradores, se deben adoptar los lineamientos establecidos por el área de Gestión Tecnológica.

Los usuarios son los únicos responsables por la seguridad de sus credenciales de acceso (usuario y contraseña), las cuales son de uso exclusivo, único e intransferible.

Para el control de acceso a la información se tiene establecidos los siguientes criterios:

Grupo de activo	Clasificación	Control de acceso a la información
Estructurada	Critica	• Información con acceso restringido, mediante asignación de roles y privilegios.
	No Critica	• Requiere control aleatorio de accesos y privilegios
No estructurada	Critica	• Información con acceso restringido, mediante asignación de roles y privilegios.
	No Critica	• Requiere control aleatorio de accesos y privilegios.
Medio Físico	Critica	• Información Control de Acceso restringido
	No Critica	• Requiere control aleatorio de accesos y privilegios.

8.2. Cuentas de los usuarios (tecnología).

No debe concederse una cuenta a personas que no sean empleados de la entidad, a menos de que estén debidamente autorizados.

Privilegios especiales tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas. Dichos privilegios deben ser ratificados cada mes con la revisión de controles de Acceso a la información documentada como instructivo GRCpl142_ClasificaciónActivosdeInformación ubicado en la base de conocimiento de Gestión Tecnológica de GLPI.

El área de Gestión Tecnológica realizará cada mes la ejecución de script descrito en el manual GRCpl142_ClasificaciónActivosdeInformación ubicado en la base de conocimiento de Gestión Tecnológica de GLPI, para la revisión de los derechos de acceso de los usuarios en los sistemas de información, donde compartirá evidencia a los jefes inmediatos para la revisión de derechos de acceso de sus colaboradores.
Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad de 30 días.
La solicitud de creación de cuenta de red debe realizarse por la Plataforma de Requerimientos e Incidentes GLPI cuando es personal nuevo, el cual determina los roles y privilegios que deben asignarse.

Las contraseñas o los mecanismos de acceso a los recursos informáticos que les sean otorgados a los usuarios, son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona, a menos de que exista un requerimiento legal o medie un procedimiento de custodia de claves. De acuerdo con lo anterior, los usuarios no deben

tener contraseñas u otros mecanismos de acceso de otros usuarios que puedan permitirles un acceso indebido.

Se prohíbe el uso de cuentas anónimas o de invitado en los aplicativos administrativos. Los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que los administradores de los servidores y sus respectivos sistemas operativos deben entrar empleando su propio nombre de usuario (usuario).

Toda cuenta debe ser suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 90 días el cual es reportado de manera semanal a traves del correo o grupo it@personalsoft.com.co.

Para prevenir ingresos no autorizados o ataques, el número de intentos de ingresos con una contraseña, debe limitarse a 3, luego de lo cual la cuenta involucrada queda suspendida.

Ningún colaborador debe tener la clave de administrador de los equipos de escritorio, de detectarse se debe cambiar, por lo tanto, se deberá informar al Coordinador de Gestión Tecnológica para el cambio.

Para evitar el uso no autorizado, abuso, fraude u otro acto mal intencionado que involucre los sistemas informáticos, se deben llevar logs de auditoría que contengan información detallada de las actividades realizadas.

Los archivos de bitácora (logs) y los registros de auditoría que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, son importantes para la detección de intrusos, brechas en la seguridad, investigaciones y otras actividades de auditoría. Por tal razón deben protegerse para que nadie los pueda alterar y sólo pueden ser consultados por personas debidamente autorizadas.

8.3. Estándares de perfiles de acceso.

En Personalsoft S.A.S 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	Descripción	Navegación	Área y/o Perfil
Rol administrador	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	Navegación Platino	Gestión Tecnológica: - Coordinador. - Analistas.
Rol Proveedor	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. - Administración Plataforma – Administración Antivirus - Administración Conectividad	Navegación Platino	Gestión Tecnológica: - Proveedor. - Analistas. - Aplicaciones. - Conectividad.
Rol Usuario (Colaborador)	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.	Navegación Gold Navegación Plata	Gerencia Talento Humano: - Coordinador. - Analistas. Gerencia Operaciones: - Director ISW. - Coordinador. - Director de Arquitectura. Gerencia Administrativa y Financiera: - Coordinador. - Analistas.

Tipo de perfil de Acceso	Descripción	Navegación	Área y/o Perfil
	• 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.		
Rol Múltiple	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.	Navegación Bronce	Gerencia Operaciones: - Aprendices.

8.4. Gestión de contraseñas de usuarios.

Se establece el uso de contraseñas individuales para determinar las responsabilidades de su administración.

Los usuarios pueden elegir y cambiar sus claves de acceso periódicamente, inclusive antes de que la cuenta expire.

Las contraseñas deben contener Mayúsculas, Minúsculas, números y por lo menos un carácter especial y de una longitud mínima de 8 caracteres.

El sistema debe obligar al usuario a cambiar la contraseña por lo mínimo 1 vez cada 42 días.

Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministrada por el área de Gestión Tecnológica.

Se tiene establecido un registro de las 3 últimas contraseñas utilizadas por el usuario, el cual no permite la reutilización de las mismas.

Todos los usuarios deben dar buen uso a las claves de acceso suministradas y no deben escribirlas o dejarlas a la vista.

No prestar, divulgar o difundir la contraseña de acceso asignadas a compañeros, jefes u otras personas que lo soliciten.

Todos los usuarios deben dar cumplimiento a las políticas de gestión y seguridad de la información de uso y selección de las contraseñas de acceso, por lo tanto, son responsables de cualquier acción que se realice utilizando el usuario y contraseña asignados.

Reportar a la Gestión Tecnológica sobre cualquier incidente o sospecha de que otra persona esté utilizando su contraseña o usuario asignado.

El acceso a Bases de Datos, Servidores y demás componentes tecnológicos de administración de la Plataforma y Sistemas de Información, debe estar autorizado por el área de Gestión Tecnológica.

No utilizar la opción de almacenar contraseñas en Internet.

Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la entidad, pudiendo ser causal de despido.

Siempre que se detecte un ingreso no autorizado al sistema de información, los colaboradores del sistema deben cambiar inmediatamente cada una de sus contraseñas en el sistema.

Las contraseñas no se divulgan por medio de líneas telefónicas, se envían por correo electrónico, y el usuario debe cambiarla de manera inmediata al ingresar por primera vez a aplicativo.

9. Transferencia e intercambio de información.

Los mensajes enviados a través de cualquier medio electrónico que contengan información pública, controlada o reservada, deben ir cifrados y se debe asegurar porque sólo sean conocidos por el emisor y por el receptor(es), del mensaje.

Cada área y/o supervisor de los contratos firmados con terceros, está en la obligación de verificar la firma de los acuerdos de confidencialidad previo a la transferencia de información entre la Organización y sus proveedores y/o contratistas.

Las terceras partes involucradas se verán obligadas a firmar los formatos de confidencialidad aplicables. Estos formatos están disponibles en el Portal SIG de la organización, según corresponda para los colaboradores, Proveedores y/o Terceros.

Cada jefe inmediato será el responsable de definir los permisos de acceso a los dispositivos de almacenamiento central o file server como repositorio de información organizacional.

El área de Gestión Tecnológica será el encargado de definir los mecanismos y lineamientos de uso de la unidad de almacenamiento File Server o servidor de información.

Los colaboradores y/o contratistas no deben revelar o intercambiar información confidencial de la organización por ningún medio, sin contar con la debida autorización.

La recepción de correspondencia rotulada como "Información Confidencial" únicamente podrá ser revisada y visualizada por el destinatario de los documentos.

El envío de correspondencia rotulada como "Información Confidencial" solo podrá salir de la organización en medio impreso o digital con la expresa autorización del emisor.

Los datos se compartirán con entidades terceros, proveedores y/o externos utilizando alguno de los siguientes métodos:

- Direcciones de correo electrónico oficiales o públicas.
- Protocolo seguro de transferencia de archivos (SFTP), especialmente cuando el archivo de datos sea grande y no pueda enviarse como archivo adjunto.
- Red privada virtual (Virtual Private Network, VPN) para ciertos usuarios externos autorizados en el caso de informes previamente aprobados.

10. Almacenamiento de la información y protección de los registros.

El almacenamiento se refiere a las condiciones del sitio (físico o electrónico) donde se guarda la información para garantizar su preservación. Las directrices para el almacenamiento de información son:

- El almacenamiento de la información debe asegurar el control de acceso, preservación y disponibilidad de la información.

- La responsabilidad por el almacenamiento es directamente del propietario de la información.

- Cada área o proceso de la organización debe disponer de un sitio de almacenamiento apropiado para la información crítica con restricción de acceso físico mediante cerraduras u otras opciones tecnológicas apropiadas.

11. Gestión y disposición de medios removibles.

Todos los dispositivos y unidades de almacenamiento removibles, tales como cintas, CD's, DVD's, dispositivos personales "USB", discos duros externos, cámaras fotográficas, cámaras de video, celulares, entre otros, deben ser controlados desde su acceso a la red de Personalsoft y uso hasta finalización de su contrato o cese de actividades.

El uso de medios removibles (Dispositivos USB, Discos Duros portables, CD, DVD, Blu-ray, etc.) en Personalsoft está restringido en sentido de escritura de información, los medios removibles no están autorizados como opción de respaldo de información.

Todos los equipos de la organización cuentan con políticas de DLP (Data Loss Protección), el cual realiza bloqueo de los puertos USB y medios extraíbles de información a través del endpoint de antivirus.

En caso de un colaborador requerir permisos USB, el jefe inmediato debe solicitar los permisos a través de un GLPI justificando la necesidad de uso e indicando el tiempo para la activación de estos permisos.

El uso de medios removibles solamente es autorizado a los colaboradores y/o proveedores con el aval del área de Gestión Tecnológica.

El manejo de la información organizacional en medios removibles está expuesta a riesgos, como pérdida, fuga o modificación, que compromete no solamente la información sino también la infraestructura tecnológica de Personalsoft, por lo tanto, el colaborador que los use será quien asuma las sanciones de ley aplicables en esta materia, siendo responsable de la seguridad del tipo y el tiempo de uso de la Información en estos medios.

Es responsabilidad de cada colaborador, proveedor y/o contratista que utilice medios de almacenamiento removible, tomar las medidas de resguardo necesarias sobre estos activos, con el fin de evitar accesos no autorizados, daños, perdida de información o del activo mismo, por lo tanto, será el responsable de la información en los medios removibles en todo momento y lugar.

Todo medio de almacenamiento removible usado en las estaciones de trabajo de Personalsoft debe ser escaneado mediante el software de antivirus suministrado por la organización.

Los medios de almacenamiento removibles como discos duros, y dispositivos USB, que contengan información organizacional, deben ser controlados (utilizar extracción segura, no forzar los conectores, escaneo con antivirus y desconectar el dispositivo cuando no se use) y físicamente protegidos (contra humedad, campos magnéticos, polvo y golpes).

Los medios de almacenamiento removibles deben ser de uso temporal y el colaborador deberá transferir la información organizacional a los medios que Personalsoft ha establecido para este propósito (computadores, NAS, file-server u google-drive).

Las fechas para el manejo de la información en medios removibles no podrán superar las fechas de vinculación laboral o contractual con Personalsoft.

Cuando el Colaborador considere que ya no es requerida la información organizacional guardada en el medio removible, o en caso de que su vinculación laboral o contractual haya finalizado, deberá realizar borrado de la información contenida en éste.

12. Backup´s o copias de seguridad.

Para respaldo de información, Backups o copias de seguridad, se cuenta con una política general la cual está publicada en el Portal SIG como (DR_backup) con el objetivo de establecer para los usuarios y área de Gestión tecnológica sus responsabilidades sobre las políticas de copias de seguridad.

El área de Gestión Tecnológica realizará de manera periódica la ejecución de recuperación de información de los servicios de almacenamiento como PSDATOS, FILE SERVER, NAS, etc.

13. Destrucción de la información.

La destrucción de la información, se realiza considerando los tiempos de retención del activo de información y/o información física.

Cuando un equipo de cómputo sea reasignado o dado de baja, se debe realizar una copia de respaldo de la información que se encuentre almacenada. Posteriormente debe ser sometido al procedimiento de borrado seguro GRCin31_EjecuBorradoSeguro de la información y del software instalado, con el fin de evitar pérdida de la información o recuperación no autorizada de la misma.

El área de Gestión Tecnológica, al momento de recibir un equipo la destrucción, debe ser tal que no permita la reconstrucción de la información y este se realiza una vez se entrega el equipo al área de gestión tecnológica, el cual ellos proceden con la reinstalación del sistema operativo.

14. Documentación física o en papel.

La eliminación de la información física o en papel debe ser autorizada, debe realizarse exclusivamente cuando se han obtenido los permisos correspondientes, tanto de entidades externas como de la propia organización.

La eliminación se debe realizar de forma apropiada, deben utilizarse métodos que garanticen que la información no pueda recuperarse o reconstituirse. Por ello, es importante que junto con los documentos originales se eliminen todas las copias en poder de Personalsoft, cualquiera sea su soporte o ubicación.

La eliminación debe ser segura y confidencial. Para ello, deberán utilizarse métodos con un nivel de seguridad equiparable a aquel con el que se manejaban los documentos mientras estos se encontraban en uso activo, preservándose la confidencialidad de su información.

Para cada medio en el que se puede presentar la información las directrices de destrucción incluyen:

Medio	Método de destrucción	Autorización	Registro	Responsable
Electrónicos	Borrado Lógico	Jefe inmediato/ Cliente	GLPI	Gestión Tecnológica
Física o papel	Trituración	Gerente de proyecto/ Cliente	Acta de cierre del proyecto	Gestión Administrativa y Financiera / Gestión Comercial

15. Gestión, administración y conservación documental.

La documentación de la organización es producto y propiedad de Personalsoft, y ésta ejercerá el pleno control de sus recursos informativos. Los archivos públicos, por ser un bien de uso público, no son susceptibles de enajenación.

Personalsoft garantizará el derecho a la intimidad personal y familiar, honra y buen nombre de las personas y demás derechos consagrados en la Constitución y las Leyes.

16. Política de escritorio y pantalla limpia.

El escritorio de trabajo de todos los colaboradores, de la organización, deben permanecer completamente despejado y libre de documentos controlados y/o reservados a la vista del público**.**

El escritorio o la pantalla de inicio del computador, tableta, escritorio virtual o cualquier dispositivo que permita el acceso a información organización, debe permanecer libre de documentos, carpetas e íconos de acceso directo a archivos y/o carpetas que contengan documentos. En lo posible, sólo deben permanecer en la pantalla los íconos por defecto del sistema operativo instalado en el equipo.

Todos los colaboradores y/o proveedores son responsables de velar por la adecuada protección de la información física y lógica al ausentarse de su puesto de trabajo.

17. Seguridad física y del entorno.

Para evitar accesos físicos no autorizados a las instalaciones de procesamiento de información, cuartos técnicos, que atenten contra la confidencialidad, integridad o disponibilidad de la información de Personalsoft, se cuenta con los siguientes puntos para el cumplimiento de la política.

17.1. Perímetro de seguridad física.

Todas las entradas que utilizan sistemas de control de acceso deben permanecer cerradas y es responsabilidad de todos los, Colaboradores y Terceros autorizados evitar que las puertas se dejen abiertas.

Todos los visitantes, sin excepción, deben portar la tarjeta de identificación de visitante o escarapela en un lugar visible mientras permanezcan en un lugar dentro de las instalaciones de Personalsoft.

Los visitantes deben permanecer acompañados de un Colaborador de Personalsoft, cuando se encuentren en las oficinas o áreas donde se maneje información.

Es responsabilidad de todos los, Colaboradores y Terceros de Personalsoft borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo. Igualmente, no se debe dejar documentos o notas escritas sobre las mesas al finalizar las reuniones.

El horario autorizado para recibir visitantes en las instalaciones de Personalsoft es de 7:00 AM a 6:00 PM. En horarios distintos se requerirá de la autorización del Gerente o Coordinador Administrativo.

Las instalaciones de Personalsoft se encuentran dotadas de un circuito cerrado de TV con el fin de monitorear y registrar las actividades de Colaboradores y Terceros y visitantes.

17.2. Controles de acceso físico.

Las áreas seguras, dentro de las cuales se encuentran el cuarto técnico, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y controles de acceso adecuados para la protección de la información.

En las áreas seguras, bajo ninguna circunstancia se puede fumar, comer o beber.

Las actividades de limpieza en las áreas seguras deben ser controladas y supervisadas por el área Administrativa y Financiera. El personal de limpieza se debe capacitar acerca de las precauciones mínimas a seguir durante el proceso de limpieza y se prohíbe el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.

17.3. Ubicación y protección de los equipos.

Las plataformas tecnológicas (Hardware, software y comunicaciones) debe contar con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados. Se debe instalar sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así mismo, se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.

EL acceso al Data Center contratado como servicio de Collocation por Personalsoft, se encuentra restringido por las políticas del Proveedor y solo tendrán acceso las personas registradas por el área de Gestión Tecnológica (Coordinador, Analistas).

17.4. Seguridad de los equipos fuera de las instalaciones.

Los equipos portátiles que contengan información clasificada como CONFIDENCIAL o RESERVADA, deben ser controlados mediante el almacenamiento de la información el servidor de archivos PSDATOS ó utilizando la herramienta definida por el área de Gestión Tecnológica.

Los equipos portátiles no deben estar a la vista en el interior de los vehículos. En casos de viaje siempre se debe llevar como equipaje de mano. En caso de pérdida o robo de un equipo portátil se debe informar inmediatamente al área Administrativa y Financiera y a el área de Gestión Tecnológica y debe poner la denuncia ante las autoridades competentes y debe hacer llegar copia de la misma.

Para el caso de los equipos que cuentan con puertos de transmisión y recepción de infrarrojo y Bluetooth estos deben estar deshabilitados.

17.5. Seguridad en la reutilización o eliminación de los equipos.

Cuando un equipo de cómputo sea reasignado o dado de baja, se debe realizar una copia de respaldo de la información que se encuentre almacenada. Posteriormente debe ser sometido al procedimiento de borrado seguro de la información y del software instalado, con el fin de evitar pérdida de la información o recuperación no autorizada de la misma.

18. Gestión de cambios.

Asegurar que los cambios a nivel de infraestructura, aplicaciones y sistemas de información realizados en Personalsoft se realicen de forma controlada. A continuación, se establecen procedimientos para el control de cambios ejecutados.

Toda solicitud de cambio en los servicios de procesamiento de información de Personalsoft, se debe realizar a través de un requerimiento en la herramienta del GLPI solicitando el Procedimiento de gestión de requerimientos e incidentes, con el fin de asegurar la planeación del cambio y evitar una afectación a la disponibilidad, integridad o confidencialidad de la información.

Se debe llevar una trazabilidad del control de cambios solicitados.

En el procedimiento de gestión de cambios se debe especificar los canales autorizados para la recepción de solicitudes de cambios, como el área de Gestión Tecnológica, correo electrónico, almacenamiento en la nube autorizado por Gestión Tecnológica.

Se debe establecer y aplicar el procedimiento formal para la aprobación de cambios sobre sistemas de información existentes, como actualizaciones, aplicación de parches o cualquier otro cambio asociado a la funcionalidad de los sistemas de información y componentes que los soportan, tales como el sistema operativo o cambios en hardware.

Se deben especificar en qué momento existen cambios de emergencia en la cual se debe garantizar que los cambios se apliquen de forma rápida y controlada.

Los cambios sobre sistemas de información deben ser planeados para asegurar que se cuentan con todas las condiciones requeridas para llevarlo a cabo de una forma exitosa y se debe involucrar e informar a los Colaboradores, áreas de la organización o Terceros que por sus funciones tienen relación con el sistema de información.

Previo a la aplicación de un cambio se deben evaluar los impactos potenciales que podría generar su aplicación, incluyendo aspectos funcionales y de seguridad de la información, estos impactos se deben considerar en la etapa de planificación del cambio para poder identificar acciones que reduzcan o eliminen el impacto.

Los cambios realizados sobre sistemas de información deben ser probados para garantizar que se mantiene operativo el sistema de información, incluyendo aquellos aspectos de seguridad de la información del sistema y que el propósito del cambio se cumplió satisfactoriamente.

Se debe disponer de un plan de roll-back en la aplicación de cambios, que incluyan las actividades a seguir para abortar los cambios y volver al estado anterior.

19. Protección contra código malicioso.

Se establecen las medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos en Personalsoft.

Toda la infraestructura de procesamiento de información de Personalsoft, cuenta con un sistema de detección y prevención de intrusos, herramienta de Anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos.

Se debe restringir la ejecución de aplicaciones y mantener instalado y actualizado el antivirus, en todas las estaciones de trabajo y servidores de Personalsoft.

Todos los Colaboradores y/o Terceros que hacen uso de los servicios de la Organización, el área Gestión Tecnológica son responsables del manejo del antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos, removibles, archivos, correo electrónico que estén utilizando para el desempeño de sus funciones laborales.

Personalsoft cuenta con el software necesario como antivirus para protección a nivel de red y de estaciones de trabajo, contra virus y código malicioso, el servicio es administrado por el área de Gestión Tecnológica.

Los antivirus adquiridos por la Personalsoft, sólo deben ser instalados por los responsables del área de Gestión Tecnológica.

Los equipos de terceros que son autorizados para conectarse a la red de datos de Personalsoft deben tener antivirus y contar con las medidas de seguridad apropiadas.

Todos los equipos conectados la red de Personalsoft pueden ser monitoreados y supervisados el área de Gestión Tecnológica.

Se debe mantener actualizado a sus últimas versiones funcionales las herramientas de seguridad, incluido, motores de detección, bases de datos de firmas, software de gestión del lado cliente y del servidor, etc.

Se debe hacer revisiones y análisis periódicos del uso de software no malicioso en las estaciones de trabajo y servidores. La actividad debe ser programada de forma automática con una periodicidad semanal y su correcta ejecución y revisión estará a cargo del área de Gestión Tecnológica.

Personalsoft debe contar con controles para analizar, detectar y restringir el software malicioso que provenga de descargas de sitios web de baja reputación, archivos almacenados en medios de almacenamiento removibles, contenido de correo electrónico, etc.

Se deben hacer campañas de sensibilización a todos los, Colaboradores y/o terceros de ser el caso de Personalsoft, con el fin de generar una cultura de seguridad de la información entre los Colaboradores y/o Terceros de la organización.

Los Colaboradores y/o Terceros de Personalsoft pueden iniciar en cualquier momento un análisis bajo demanda de cualquier archivo o repositorio que consideren sospechoso de contener software malicioso. En cualquier caso, los Colaboradores y/o Terceros cuando sea necesario siempre podrán consultar al área de Gestión Tecnológica sobre el tratamiento que debe darse en caso de sospecha de malware.

Los usuarios no podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus o de detección de código malicioso, en los equipos o sistemas asignados para el desempeño de sus funciones laborales.

Todo usuario es responsable por la destrucción de archivos o mensajes, que le haya sido enviado por cualquier medio provisto por la Personalsoft, cuyo origen le sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, el usuario debe reenviar el correo a la cuenta it@personalsoft.com.co.

El área de Gestión Tecnológica tiene el derecho de monitorear las comunicaciones y/o la información que se generen, comuniquen, transmitan o trasporten y almacenen en cualquier medio, en busca de virus o código malicioso.

El área de Gestión Tecnológica se reserva el derecho de filtrar los contenidos que se trasmitan en la red de Personalsoft, con el fin de evitar amenazas de virus.

20. Instalación de software.

Las normas de protección de la propiedad intelectual obligan a las empresas a usar en todo momento software legal. El uso de software pirata o adquirido de forma fraudulenta podría conllevar sanciones económicas y penales.

En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de información, únicamente se permite la instalación de software con licenciamiento apropiado y acorde a la propiedad intelectual y bajo aprobación del área de Gestión Tecnológica.

El área de Gestión Tecnológica es la responsable de brindar asesoría y supervisión para la instalación de software especializado.

Es responsabilidad de cada colaborador el buen uso del software que se encuentra instalado en el equipo de cómputo asignado para el desarrollo de sus funciones.

El área de Gestión Tecnológica debe revisar con regularidad el software que se encuentra instalado en los equipos de cómputo de la entidad y tiene la protestad de desinstalar el software clasificado como inadecuado o que vulnere la seguridad de los recursos de red o que viole los derechos de autor.

Los colaboradores no deben introducir intencionalmente software diseñado para causar daño o impedir el normal funcionamiento de los sistemas de información, por lo tanto, cada usuario es responsable de lo que pueda hacer o la información que pueda generar en los sistemas de información.

El área de Gestión Tecnológica es la responsable de controlar y verificar la utilización de software en los equipos de cómputo.

Por lo anterior, todos los colaboradores, que usen activos de información que sean propiedad de Personalsoft, son responsables de cumplir y acoger con integridad nuestra política de Activos Fijos (SAFdr03_Política Activos Fijos), la cual puede se ser consultada en el Portal SIG

21. Equipos de comunicación switches y routers.

El área de Gestión Tecnológica es absolutamente responsable del manejo de los dispositivos de red entiéndase por Routers y Switches AP (Access Point) de los que dispone Personalsoft, velando porque estén dispuestos en lugares seguros y protegidos a

nivel físico, así como también a nivel lógico el cual se menciona a continuaciones los controles para estos:

Las contraseñas predefinidas que traen los dispositivos nuevos, deben cambiarse inmediatamente al ponerse en servicio el dispositivo.

Se deberá designar al personal que efectuará las actividades de instalación, desinstalación, mantenimiento y conexión física de estos dispositivos.

Se deberán enumerar protocolos, puertos y servicios a ser permitidos o filtrados en cada interface, así como los procedimientos para su autorización.

Se deberán identificar los servicios de configuración dinámica de los Routers, y las redes permitidas para acceder a dichos servicios.

Se deben tener plenamente identificados los protocolos de ruteo a utilizar, y los esquemas de seguridad que proveen Seguridad en el Router.

22. **Equipos de impresoras.**

En PersonalSoft para el uso de dispositivos de impresoras o servicios de impresión y un correcto uso se definen los siguientes controles:

Los documentos que se impriman en las impresoras de Personalsoft deben ser de carácter organizacional.

Al imprimir documentos de carácter CONFIDENCIAL, estos deben ser retirados de la impresora inmediatamente. Así mismo, no se deben reutilizar papel que contenga información CONFIDENCIAL.

Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión para que no se afecte su correcto funcionamiento.

Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar al área de Gestión Tecnológica.

23. Registro de auditoria y supervisión.

Los Recursos de Información críticos deben disponer de mecanismos que alerten sobre eventos que comprometan su integridad, confidencialidad y/o disponibilidad. Deben existir herramientas de generación de alertas en tiempo real a nivel de hardware, sistema operativo, software de administración y/o software de seguridad, las cuales deben ser habilitadas en concordancia con la clasificación y criticidad del recurso informático.

Los registros de los eventos deben ser protegidos contra manipulación y acceso no autorizado de acuerdo con ellos.

Personalsoft realizará un monitoreo permanente de la red a través de los diferentes Logs establecidos y configurados a conveniencia del negocio. Estos Logs serán revisados y analizados de acuerdo con las tareas programadas dentro del área de Gestión Tecnológica.

Este registro será almacenado en el servidor PSVM de Personalsoft, cada vez que sea ejecutado y revisado para efectos de evidencias.

Se deben registrar de manera permanente y revisar continuamente las actividades de usuarios privilegiados como los Administradores de Recursos de Información, Instaladores de Software, Operadores, Administradores de Control de Acceso Lógico, etc.

La fecha y la hora deberán estar sincronizadas en todos los Recursos de Información de acuerdo con un estándar, para asegurar que los registros reflejan el tiempo exacto de ocurrencia. En el caso de que se trate de Recursos de Información ubicados en el exterior, se deben tener en cuenta las diferencias horarias.

24. Desarrollo de software seguro.

La Política de Desarrollo Seguro de Personalsoft comprende las reglas para el desarrollo de software y sistemas dentro de la organización. Para esto, se establecen los siguientes lineamientos:

- Se deberán utilizar técnicas de programación seguras tanto para los desarrollos nuevos como en las situaciones de reutilización de códigos donde es posible que no se conozcan las normas que se aplican al desarrollo o donde no sean coherentes con las buenas prácticas actuales. Lo anterior, tanto para el desarrollo interno como externo.

- Se debe estandarizar el ciclo de vida del desarrollo de software en la CNE, logrando con ello los siguientes objetivos:

    - Definir actividades a llevarse a cabo en un proyecto de desarrollo de software.
    - Unificar criterios en la organización para el desarrollo de software.
    - Proporcionar puntos de control y revisión.
    - Se deben estandarizar, los criterios de seguridad y calidad, que serán considerados, durante cada fase del proceso de desarrollo de sistemas de información.
    - En cuanto al desarrollo de sistemas por terceros, se deben celebrar contratos, con las empresas proveedoras, que contengan cláusulas, que resguarden la propiedad intelectual para Personalsoft, y así mismo, aseguren, los niveles de confidencialidad de la información, en el proyecto respectivo.
    - Se debe diferenciar, entre el encargado de celebrar y autorizar los contratos con terceros, de los que deben fiscalizar su cumplimiento.

25. Gestión de vulnerabilidades técnicas.

Se debe realizar como mínimo dos veces al año escaneo de vulnerabilidades técnicas a todos los componentes tecnológicos que se encuentren en la red de PersonalSoft

Es responsabilidad de la Gerencia de Tecnología mantener un esquema de pruebas de vulnerabilidad a los componentes de la red dependiendo del análisis de riesgos.

Todo integrante de la entidad es responsable por reportar en forma inmediata cualquier condición anormal o vulnerabilidad que detecte en el uso los Recursos de Información de PersonalSoft

La información específica sobre las vulnerabilidades o condiciones anormales de seguridad de la información tiene carácter restringido y solo debe darse a conocer a personas autorizadas y que tengan una necesidad demostrada de saberlo.

La instalación de software debe ser previamente autorizado y debe cumplir con los requerimientos legales que faciliten su utilización, sólo podrá ser el autorizado por la Gerencia Tecnología de PersonalSoft

La Compañía efectuará constantes revisiones al cumplimiento de las normas en materia de propiedad intelectual. Los colaboradores y/o terceros tienen PROHIBIDO instalar o utilizar software o productos no licenciados por la Compañía. Se exceptúan de esta política los productos de software con licencia de libre utilización o que sean soportados

con certificado de propiedad de licencia de terceros. En todo caso, cualquier instalación de software debe ser solicitada y obtenida a través del área de Gestión de Tecnológica.

26. Gestión de incidentes de seguridad de la información.

La gestión de incidentes de seguridad inicia desde la identificación de un posible incidente, detección, contención y solución de este, finalizando con la documentación y lecciones aprendidas, por lo cual PersonalSoft tiene establecida la Política (GRCdr31_Política Gestión de Requerimientos e Incidentes). Además establece los siguientes medios para el reporte de posibles incidentes de seguridad:

- Enviar un correo electrónico con la descripción de la situación identficada a la dirección it@personalsoft.com.co

- Ingresar al módulo de PQRS de la página corporativa personalsoft.com https://www.personalsoft.com/index.php/es/escribenos/peticiones-quejas-y-reclamos.html

- Llamar al número telefónico +57 (4) 4037250 y a la extensión IP 301 de Gestión Tecnológica.

- El colaborador que identifique el posible incidente de seguridad debe reunir la información que llevó a determinar que es un posible incidente, la cual podrá ser utilizada en la atención del mismo, Ejemplo: capturas de pantalla, correos electrónicos, fotografías, videos entre otros.

Una vez se reciba la notificación telefónicamente o a través de correo electrónico de un posible incidente de seguridad, el área de Gestión Tecnológica debe realizar la primera categorización en el GLPI para iniciar con la atención del mismo, allí se generará un ticket /número de servicio de acuerdo a los siguientes criterios básicos:

- Hubo daño o pérdida de información.

- Hubo fuga y/o robo de información.

- Hubo robo de credencias o información mediante Phishing.

- Se presentó modificación no autorizada de la información.
- Comportamiento anormal del computador y/o sistema de información.
- Se presentó suplantación de identidad.
- Se presentó un acceso no autorizado.
- Se presentó pérdida o alteración de registros de base de datos.
- Se presentó una pérdida de un activo de información.
- Hubo presencia de código malicioso “malware, ransomware”.
- Se presentó una denegación del servicio.
- Se presentó algún ciberataque.

27. Aplicabilidad.

El contenido de este documento aplica a todos los procesos y procedimientos que conforman el Sistema Integrado de Gestión de Personalsoft, así como a todas las actuaciones administrativas que desarrollen las distintas áreas, por intermedio de sus colaboradores, proveedores y/o contratistas.

Se sancionará disciplinaria, administrativa, civil y/o penalmente a toda persona que viole las disposiciones del presente documento de conformidad con lo establecido en las leyes colombianas vigentes.