MANUAL DE POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

ASEGURAMIENTO DE LA GESTIÓN / GESTIÓN INTEGRAL DE RIESGOS

TABLA DE CONTENIDO

1. Objetivo 5
2. Alcance 5
3. Definiciones 5
4. Políticas 8
4.1. Política de control de acceso 8
4.1.1 Identificación de usuarios 9
4.1.2 Autenticación de usuarios 10
4.1.3 Autorización de accesos 11
4.1.4 Control de accesos basado en roles 12
4.1.5 Privilegios de acceso en la administración de recursos tecnológicos 13
4.1.6 Registro y auditoría de accesos 13
4.1.7 Gestión del ciclo de vida de los accesos 14
4.1.8 Revisión periódica de accesos 15
4.1.9 Gestión de usuarios privilegiados 16
4.1.10 Usuarios de servicio 16
4.2 Política de Seguridad de la Información para las relaciones con proveedores 17
4.2.1 Etapa precontractual 17
4.2.2 Etapa contractual 19
4.2.3 Etapa post contractual 20
4.3 Política Seguridad de la Información en los recursos humanos 21
4.4 Política de gestión de activos de información 22
4.4.1 Consideraciones generales 22
4.4.2 Modificación directa sobre Base de datos en producción 24
4.5 Política de uso aceptable de activos de información 25
4.6 Política seguridad física y ambiental 26

4.6.1. Trabajo en áreas seguras 26
4.6.2 Controles físicos de ingreso a las instalaciones y a las áreas restringidas 28
4.7 Política seguridad de las operaciones 29
4.8 Política de seguridad en las comunicaciones digitales 30
4.9 Política para adquisición, desarrollo y mantenimiento de sistemas de información 31
4.10 Política de gestión de incidentes de Seguridad de la Información 33
4.10.1 Obligación de reporte y gestión 33
4.10.2 Preparación para la gestión de incidentes 35
4.10.3 Equipo de respuesta a incidentes (ERI) 36
4.10.4 Clasificación y priorización de incidentes 36
4.10.5 Detección automática de eventos de riesgo 37
4.10.6 Gestión de incidentes 37
4.10.7 Documentación de la gestión de incidentes 37
4.10.8 Uso de evidencia digital 38
4.11 Política continuidad de la Seguridad de la Información 38
4.12 Política cumplimiento de Seguridad de la Información 39
4.13 Política dispositivos para movilidad y acceso remoto 41
4.13.1 Movilidad 41
4.13.2 Obligaciones de los usuarios de dispositivos móviles de COLPENSIONES 42
4.13.3 Dispositivos móviles provistos por COLPENSIONES 43
4.13.4 Protección para dispositivo propio 44
4.13.5 Política para la Seguridad de la Red 45
4.14 Política para la gestión de ciberseguridad 47
4.15 Política para el desarrollo seguro 48
4.16 Política para gestión de medios de almacenamiento 53
4.16.1 Gestión de medios removibles 53
4.17 Política para la concienciación en Seguridad de la Información y ciberseguridad 54

4.18 Política para gestión de vulnerabilidades 55
4.19 Política de gestión de cambios tecnológicos en COLPENSIONES 57
4.20 Política para el licenciamiento y uso de software 57
4.21 Política de seguridad para equipos de cómputo 58
4.22 Política de escritorio limpio y pantalla limpia 59
4.23 Política para la transferencia de información 60
4.23.1 Directrices de intercambio de información entre personal de COLPENSIONES 61
4.23.2 Directrices de intercambio de información con terceros. 61
4.24 Política de uso de controles criptográficos 61
4.25 Política de trabajo en casa – Conexión Remota Externa 62
4.25.1 Directrices de seguridad para todo el personal 62
4.25.2 Directrices de configuraciones de seguridad 63
4.26 Política de gestión de llaves criptográficas 63
4.27 Política de seguridad en la nube 64
4.28 Política de copias de respaldo 65
5. Excepciones 68
6. Incumplimiento de Políticas y Lineamientos de Seguridad de la Información y Ciberseguridad 68
7. Control de cambios del documento 69

1. Objetivo

Definir y comunicar a las partes interesadas las políticas y lineamientos de Seguridad de la Información que deben ser aplicados por parte de todos los colaboradores de COLPENSIONES y las partes interesadas, con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad, tomando como referencia la Norma ISO/IEC 27001:2013 y su anexo A.

2. Alcance

Las políticas definidas en el presente documento aplican para todos los procesos de la Entidad y las partes interesadas que acceden, almacenan, distribuyen y/o eliminan información de COLPENSIONES; las partes interesadas se describen en el documento AGE-GIR-DIN-OO8 - Grupos de Interés Sistema de Gestión de Seguridad de la Información y Ciberseguridad

3. Definiciones

A continuación, se presenta la definición de algunos términos que se utilizan en el desarrollo del documento:

1. **Activo de Información:** Cualquier elemento que contenga, datos que tienen valor para uno o más procesos de la organización y debe protegerse. (ISO/IEC 27001:2013).
2. **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión conservados, respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. (Archivo General de la Nación, 2006).
3. **Ataque:** Intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo (ISO/IEC 27000:2018).
4. **Bluetooth:** Protocolo de comunicaciones que sirve para la transmisión inalámbrica de datos (fotos, música, contactos…) entre diferentes dispositivos que se hallan a corta distancia.
5. **Ciberseguridad:** se entiende como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales. (Conpes 3995).
6. **Cifrado fuerte:** El cifrado implica convertir texto sin formato legible por humanos en un texto incomprensible, conocido como texto cifrado. Los dos métodos de cifrado más comunes son el cifrado simétrico y el cifrado asimétrico. Los nombres hacen referencia a si se utiliza o no la misma clave para el cifrado y el descifrado. (KASPERSKY)

7. **Colaborador:** Con este nombre se hace referencia a la persona que tiene cualquier tipo de vínculo contractual, legal y reglamentario con COLPENSIONES, esto incluye trabajadores públicos, oficiales, personal contratado directamente, proveedores, contratistas, estudiantes en práctica, trabajadores en misión, estudiantes en pasantía y cualquier persona a la que le sea asignada una responsabilidad por parte de COLPENSIONES.
8. **Computación en la nube:** Modelo mediante el cual se habilita el acceso a recursos de procesamiento y almacenamiento de información a través de una red (habitualmente internet), de manera escalable y flexible, permitiendo el auto aprovisionamiento y administración.
9. **Confidencialidad:** Propiedad de la información que garantiza no estar disponible o ser divulgada a personas, Entidades o procesos no autorizados. (ISO/IEC 27000:2018).
10. **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de Seguridad de la Información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. (MinTIC- Modelo de Seguridad y Privacidad de la Información 2016).
11. **Control de acceso:** Garantizar que el acceso a los activos esté autorizado y restringido según los requisitos de negocio y de seguridad. (ISO/IEC 27000:2018)
12. **CVE (Vulnerabilidades y exposiciones comunes):** lista de vulnerabilidades y exposiciones de seguridad de la información.
13. **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012).
14. **Disponibilidad:** Propiedad de la información que garantiza el ser accesible y usable de acuerdo con lo requerido por una Entidad autorizada. (ISO/IEC 27000:2018).
15. **Equipo de cómputo:** Dispositivo electrónico para procesamiento de información controlado por programas de software.
16. **Etiquetar / Marcar:** Procedimiento mediante el cual se rotula un activo de información físico o digital utilizando una convención que identifica su clasificación para confidencialidad, integridad y disponibilidad. El término “etiquetar”, al cual hace referencia la Norma ISO 27001:2013, se cambia para efectos del presente documento por “marcar”, lo anterior teniendo en cuenta que el Proceso de Gestión Documental adoptó el término “etiquetar” con una connotación diferente.
17. **Evento de Seguridad de la Información:** Ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información o falla
18. **Firewall (cortafuego):** Dispositivo de seguridad de red que supervisa el tráfico de red entrante y saliente y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.
19. **Fuente autoritativa:** Repositorio con el registro de usuarios el cual constituye la fuente raíz para la identificación de las identidades de los colaboradores para la autorización de acceso a la información y a los sistemas de información.

20. **Gestión de incidentes de seguridad de la información y Ciberseguridad: Procesos** para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
21. **GPS (Sistema de Posicionamiento Global):** Sistema de navegación por satélite que permite determinar en cualquier momento la posición de un objeto y/o Persona.
22. **Incidente de Seguridad de la Información:** Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información
23. **Indicador:** Medida que proporciona una estimación o evaluación (ISO/IEC 27000:2018).
24. **Integridad:** Propiedad de exactitud y completitud de la información que contienen los activos de información. (ISO/IEC 27000:2018).
25. **IDS:** Sistema de Detección de Intrusos, su función es detectar accesos no autorizados a un ordenador o a una red.
26. **IPS:** Sistema de Prevención de Intrusiones, su función es proteger a los sistemas de ataques e intrusiones. Su actuación es preventiva
27. **MAI (Matriz de Activos de Información):** Tabla en la cual se registran los activos de información de cada uno de los procesos, su caracterización y su clasificación frente a las propiedades de la Seguridad de la Información: confidencialidad, integridad y disponibilidad
28. **Matriz de riesgos de Seguridad de la Información:** Registro en el cual se describen los riesgos de Seguridad de la Información identificados en cada proceso, especificando los activos de información afectados, las causas, amenazas y consecuencias, así como su valoración
29. **Marcado:** Para efectos del Sistema de Gestión de Seguridad de COLPENSIONES, equivale al término “etiquetado” NFC (comunicación de campo cercano): Permite realizar un intercambio de datos entre dos dispositivos de manera inalámbrica
30. **NFC Near-field communication** o comunicación de campo cercano es una tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos.
31. **OWASP Open Web Application Security Project:** Está dedicado a la búsqueda y la lucha contra las vulnerabilidades en el software. La OWASP Foundation es una organización sin ánimo de lucro que proporciona la infraestructura y apoya a este trabajo
32. **Parte Interesada:** Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad. (ISO/IEC 27000:2018).
33. **Rollback:** Operación que devuelve cambios generados en los sistemas de información.
34. **Root:** Usuario privilegiado que tiene el control absoluto de todo lo que ocurre en el sistema, accediendo a todas las funciones y realizando configuraciones.
35. **Servicios:** Servicios de computación y comunicaciones, tales como los de consulta, correo electrónico, mensajería instantánea, videoconferencia, herramientas colaborativas y streaming, entre otros que sean prestados por un tercero. (Adaptado de la Guía para la Gestión y Clasificación de Activos de Información,2016).
36. **Sysadmin:** Usuario que permite la administración de los sistemas.

37. **Sistema de Gestión de Seguridad de la Información y Ciberseguridad:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una entidad para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua
38. **SOC (Centro de Operaciones de Seguridad):** Permite la supervisión y administración de la seguridad del sistema de información a través de herramientas de recogida, correlación de eventos e intervención remota.
39. **Usuario de servicio:** Cuenta que se utiliza sobre una aplicación para autenticarse sobre otra aplicación o sistema de información.
40. **Usuario Privilegiado:** Usuario con acceso o capacidades especiales por encima de las de un usuario estándar, puede asociarse tanto a usuarios humanos como a usuarios no humanos, como las aplicaciones y las identidades de las máquinas. Se tiene entre otros, los siguientes: Cuenta de superusuario / default del sistema, Cuenta administrativa de dominio, Cuenta administrativa local, Cuenta de emergencia, Usuario empresarial / funcional con privilegios.
41. **VPN:** Virtual Network protocol
42. **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotado por una o más amenazas
43. **Wifi:** Mecanismo que permite, de forma inalámbrica, el acceso a Internet de distintos dispositivos al conectarte a una red determinada.

4. Políticas

A partir de la definición de la Política General de Seguridad de la información y ciberseguridad AGE-GIR-DIN-005 que direcciona la Sistema de Gestión de Seguridad de la Información, en el presente capítulo se realiza el desarrollo políticas específicas que componen el Manual de Políticas y Lineamientos de Seguridad de la Información y Ciberseguridad, describiendo para cada una de ellas los lineamientos que deben cumplir los colaboradores de COLPENSIONES, para preservar la confidencialidad, integridad y disponibilidad de la información de la Entidad.

Como parte de la mejora continua de este documento, se debe realizar al menos una vez al año la revisión y actualización de este documento.

4.1. Política de control de acceso

La presente política describe los lineamientos para la protección de la información de accesos no autorizados, la cual debe partir de la clasificación de los activos de información y del análisis de riesgos realizados por su propietario.

4.1.1 Identificación de usuarios

El control de acceso a la información y sistemas de información de COLPENSIONES tiene como base fundamental una correcta identificación de usuarios, para lo cual se definen los siguientes puntos:

a) Para la creación e inactivación de usuarios, se debe realizar de acuerdo a lo definido en el Procedimiento *de Gestión de Accesos*. *Código GGT-PSE-CPR-001,* del proceso Gestión de Provisión del servicio TI.
b) Cada usuario tendrá asignado un identificador único para el uso de los sistemas de información y en las aplicaciones de COLPENSIONES, el cual es creado de acuerdo con las reglas establecidas en el *Procedimiento de Gestión de Accesos Código GGT-PSE-CPR-001,* del proceso Gestión de Provisión del servicio TI.
c) Un identificador de usuario no podrá ser reasignado ni reutilizado.
d) Para generar tanto acceso físico como lógico a proveedores y contratistas, el supervisor del contrato, o su superior, debe realizar la solicitud al propietario de la información, a través del mecanismo designado por el Procedimiento de Gestión de Accesos Código GGT-PSE-CPR-001
e) COLPENSIONES debe contar con una gestión de identidades centralizada, encargada de permitir o restringir el ingreso a la información por parte de los usuarios, de acuerdo con los privilegios de acceso definidos, los cuales deben corresponder a la autorización definida por su propietario. Los sistemas de información esenciales deben consultar el sistema único de control de acceso para definir los permisos con los que cuenta cada usuario.
f) La creación de cuentas es responsabilidad del proceso Gestión Provisión del Servicio de TI.
g) Cada colaborador de COLPENSIONES debe responsabilizarse de los usuarios y claves que le son asignados para el acceso a los sistemas de información y aplicaciones de la Entidad.
h) Las cuentas de usuario son personales e intransferibles.
i) Bajo ninguna circunstancia un usuario puede revelar o compartir su contraseña de acceso o acceso a alguna sesión abierta en cualquier equipo sistema de información.
j) Bajo ninguna circunstancia se puede solicitar a un colaborador el suministro de su contraseña de acceso; los colaboradores que brindan asistencia técnica (ejemplo: Mesa de Servicio, grupos de soporte técnico) nunca podrán argumentar que se requiere este dato para poder atender un requerimiento.
k) Una vez que la relación contractual del contratista o proveedor haya finalizado, el supervisor del contrato, o su superior inmediato, es responsable de solicitar al Grupo de Gestión de Accesos de la

Gerencia de Tecnologías de la Información, inmediatamente, la inactivación de los derechos de acceso a el(los) usuario(s) relacionado(s) con ese contrato de acuerdo con lo definido en el *Procedimiento de Gestión de Accesos; y verificar estas acciones sobre los servicios o aplicaciones relacionadas Código GGT-PSE-CPR-001*

l) Es responsabilidad del proceso Gestión Provisión del Servicio de TI inactivar los usuarios correspondientes al personal cuya relación contractual con COLPENSIONES o con terceros haya finalizado

4.1.2 Autenticación de usuarios

Los siguientes lineamientos describen la forma cómo se debe validar la identidad de los usuarios para asegurar que el usuario que está tratando de ingresar a la información o a un sistema de información de COLPENSIONES, es quien dice ser:

a) Los sistemas de información utilizados en COLPENSIONES, deben realizar procesos de validación de la identidad de los usuarios (autenticación) mediante uno de los siguientes factores:

- Algo que únicamente el usuario sabe: por ejemplo, contraseñas o códigos de acceso.
- Algo que únicamente el usuario posee: por ejemplo, tarjetas de proximidad, elementos físicos como llaves, dispositivos tipo Token o códigos OTP, entre otros.
- Algo que únicamente el usuario es: corresponde a la validación de características físicas o morfológicas del usuario mediante dispositivos biométricos.

b) Los métodos de autenticación y control de acceso a los sistemas de información y aplicaciones deben ser definidos por los propietarios de la información de acuerdo con el resultado del análisis de riesgos, e implementados por el proceso Gestión Provisión del Servicio de TI.

c) Los sistemas de información deben realizar la autenticación de usuarios a través del sistema que COLPENSIONES ha implementado de manera centralizada para tal fin.

d) Los sistemas de información deben seguir los lineamientos para la gestión de accesos para el inicio de sesión descritos a continuación:

- Incluir un mensaje de inicio de sesión sobre el uso aceptable del sistema, aplicación o dispositivo y sobre la necesidad de ser un usuario registrado y autorizado para poder acceder al mismo.

- Configurar las cuentas de usuario para que se bloqueen por un número de 5 intentos de ingreso fallidos para proteger el sistema de ataques de fuerza bruta.
- El proceso de autenticación debe únicamente generar mensajes de error al finalizar el proceso de validación sin dar detalles del fallo. En casos en los que se requiere más de un factor de autenticación, no se debe informar en cada paso el éxito o error de la validación.
- Evitar la entrega de información en los mensajes que guían al usuario durante el ingreso a las aplicaciones.
- Configurar el sistema para forzar que el usuario realice cambio de contraseña cuando la use por primera vez.
- Almacenar registros o logs de auditoría de los intentos exitosos y fallidos de ingreso.
- Es responsabilidad del proceso Gestión Provisión del Servicio de TI configurar opciones de control de ingreso, las cuales permitan inactivar o bloquear el acceso pasados 30 días calendario desde el último ingreso autenticado.

e) Las aplicaciones y los sistemas de información deben gestionar las sesiones de usuario contemplando los siguientes lineamientos:

- No permitir inicios de sesión concurrentes con el mismo usuario. Para el caso de usuarios privilegiados, en caso de requerirse, el propietario del sistema de información o aplicación debe autorizar el uso de sesiones concurrentes, definiendo cuál es el número máximo.
- Todos los módulos de los sistemas de información deben manejar métodos de validación de las sesiones, con el fin de verificar la autenticidad del usuario, el estado de este y las autorizaciones o permisos.
- Las sesiones de usuario deben tener un parámetro para configurar el tiempo de inactividad del usuario, el cual una vez transcurrido, deberá solicitar nuevamente la autenticación del usuario o cerrar la sesión para impedir el acceso no autorizado.

4.1.3 Autorización de accesos

El acceso a la información sólo se debe permitir si cuenta con la autorización de su propietario, para lo cual se definen los siguientes puntos:

a) El responsable de definir los controles para el acceso a la información es su propietario, y es el encargado de autorizar el acceso a sus activos de información.

b) Los custodios de los activos de información son los únicos responsables de velar porque los controles de acceso sean aplicados de acuerdo con lo establecido por el propietario correspondiente.

4.1.4 Control de accesos basado en roles

A través de los siguientes lineamientos se establece la importancia de la definición de roles, para asegurar un nivel de acceso a la información acorde con el perfil del usuario:

a) Los sistemas de información utilizados en COLPENSIONES deben permitir configurar permisos o privilegios agrupados en roles o perfiles, a través de la matriz de roles de aplicación que el proceso Provisión del Servicio de TI define y administra, considerando los siguientes criterios:

- Estar alineados con los permisos y atribuciones requeridos en las matrices de roles empresariales definidas para cada proceso.
- Permitir la asignación de permisos con base en los requerimientos del negocio.
- Aplicar los principios de menor privilegio y segregación de funciones.

b) Los líderes de proceso y jefes de área de COLPENSIONES, deben definir, documentar y mantener actualizados los roles empresariales asociados a los cargos de su proceso, identificando las necesidades de acceso a los activos de información a través de la matriz de roles empresariales. Las matrices de roles empresariales deben contener las aplicaciones o sistemas de información a los que cada cargo puede acceder, los roles asociados y los perfiles en cada una de las aplicaciones; su definición debe responder a los requerimientos de los procesos de la Entidad.

c) Las definiciones de la Matriz de Roles Empresariales: cargo, rol empresarial y perfiles, debe asegurar la aplicación de los principios de segregación de funciones y mínimo privilegio requerido.

d) Cualquier modificación que se requiera realizar sobre la definición de roles empresariales y perfiles asociados, debe ser aprobada por los propietarios de los activos de información involucrados y por el líder del proceso y/o jefe de área.

e) Se deben definir accesos por demanda a las aplicaciones, que no estén incluidos en los roles empresariales de cada área y que permitan acceder por un intervalo de tiempo definido, estos accesos deben ser solicitados a cada usuario cuando sea requerido a través la herramienta definida por la Entidad y aprobados por el propietario del sistema de información o aplicación.

f) El grupo de Gestión de Accesos de la Gerencia de Tecnologías de la información, tendrá como insumo la Matriz de Roles Empresariales, para la asignación de permisos a las aplicaciones; también gestionan accesos por demanda, los cuales serán asignados por medio de la herramienta definida por la Entidad.

4.1.5 Privilegios de acceso en la administración de recursos tecnológicos

Los recursos tecnológicos deben contar con un control que permita el acceso sólo a los usuarios autorizados; para lo anterior se definen los lineamientos descritos a continuación:

a) La Gerencia de Tecnologías de la Información debe garantizar la segregación de responsabilidades entre ambientes tecnológicos (ambientes de prueba, desarrollo y producción).
b) No se permite el acceso de personal encargado del desarrollo de aplicaciones y sistemas de información a los ambientes de producción. En caso de ser necesario, este acceso debe ser de consulta y autorizado por tiempo limitado por parte del propietario de la aplicación o sistema de información y el custodio debe asegurar los controles definidos por sus propietarios.
c) El acceso a las bases de datos productivas, sólo se puede hacer a través de las aplicaciones o sistemas de información autorizadas por la Entidad para tal fin. En caso de requerirse un acceso diferente, se debe realizar un análisis de riesgos, el custodio de la base de datos debe asegurar la implementación los controles definidos por el propietario de la información de acuerdo con este análisis, y, en cualquier caso, se debe asegurar que los únicos roles que pueden tener acceso es el de Administrador de Bases de Datos (DBA) y el Grupo de Gestión de Accesos de la Gerencia de Tecnologías de la información
d) El acceso al código fuente de las aplicaciones o sistemas de información desarrollados por COLPENSIONES, o por quien la Entidad designe para tal fin, debe ser restringido únicamente al personal encargado de los proyectos de desarrollo; cualquier acceso u operación sobre el código debe dejar los registros de auditoría necesarios. Ningún usuario que tenga un rol diferente podrá acceder a dicho código fuente ni siquiera en modo consulta o sólo lectura.

4.1.6 Registro y auditoría de accesos

La trazabilidad es un elemento de gran importancia para efectos de investigaciones y seguimiento ante un incidente de seguridad de la información; se debe asegurar lo siguiente:

a) Los sistemas de información deben dejar registros o logs de auditoría del ingreso de los usuarios y las actividades que realizan, para tal fin, la Gerencia de Tecnologías de la Información debe definir e implementar el registro de logs de las actividades de los usuarios.
b) Los registros de los sistemas de control de accesos deben ser monitoreados por la Gerencia de Prevención del Fraude de acuerdo con la criticidad de los activos de información que dichos sistemas protejan.
c) Los sistemas de información deben mostrar al usuario en cuanto sea posible, la fecha y hora de su último ingreso para facilitar la identificación de posibles incidentes de seguridad relacionados con suplantación y compromiso de credenciales de autenticación.

4.1.7 Gestión del ciclo de vida de los accesos

A continuación, se presentan los lineamientos para que el acceso a la información y sistemas de información de COLPENSIONES sea controlado de manera permanente, para evitar accesos no autorizados asociados con la creación, modificación y eliminación de cuentas de usuario y accesos:

a) Cuando la ejecución de requerimientos relacionados con accesos a aplicaciones y sistemas de información debe hacerse de forma manual, el responsable de esta tarea es el Grupo de Gestión de Accesos de la Gerencia de Tecnologías de Información.
b) El acceso a sistemas de información y aplicaciones debe ser autorizado por el Gerente o Jefe de Área, de acuerdo con los roles empresariales establecidos para el cargo, los cuales se encuentran definidos en la Matriz de Roles Empresariales.
c) Si se requiere realizar una actualización sobre la Matriz de Roles Empresariales, se debe seguir el INSTRUCTIVO GESTIÓN MATRIZ DE ROLES EMPRESARIALES - AGE-GIR-INS-050.
d) Cuando un colaborador de COLPENSIONES requiera acceso a aplicaciones o sistemas de información de un tercero, se debe seguir el Procedimiento *Gestión de Accesos* asignado al proceso Gestión de Provisión del Servicio TI. El supervisor de contrato o convenio debe asegurar que el tercero conserve un registro de los ingresos de los usuarios de COLPENSIONES a sus aplicaciones y sistemas de información, así como de las acciones ejecutadas; esto debe quedar estipulado en el contrato con el tercero.
e) Todo requerimiento para creación de usuarios, solicitud de acceso a información y novedades sobre estos usuarios y accesos que no pertenezcan a la Entidad, debe tener un responsable al interior de COLPENSIONES:

- Para los usuarios de terceros, es el supervisor del contrato.
- Para los usuarios de los entes de control, es el Gerente o Jefe de Área que tiene a cargo la responsabilidad frente al ente de control al que pertenece el usuario para el cual se solicita el acceso.

4.1.8 Revisión periódica de accesos

Los accesos a la información y sistemas de información deben validarse permanentemente para asegurar que se encuentran actualizados y corresponden a los permisos otorgados por los propietarios de la información. Se establecen los siguientes lineamientos:

a) El Propietario de la Información debe realizar revisiones periódicas para asegurar la coherencia entre los accesos otorgados, perfiles técnicos asignados y la definición de los roles empresariales de la Entidad, los cuales se deben validar frente a la fuente autoritativa.
b) La matriz de roles empresariales se debe revisar periódicamente, mínimo una (1) vez al año, o cuando por cambios en las actividades de los colaboradores o el proceso así lo requieran; la revisión debe ser realizada por parte de su propietario (registrado en la MAI) en conjunto con los líderes de proceso, jefes de área y gestores de Seguridad de la Información y Ciberseguridad, para asegurar la vigencia y aplicabilidad de la matriz.
c) Las autorizaciones de acceso privilegiado deben ser revisadas por lo menos cada tres (3) meses o cuando exista un cambio en la matriz de roles empresariales, que implique modificaciones sobre un acceso de este tipo.
d) Todas las cuentas de usuario que no hayan presentado actividad de inicio de sesión en los sistemas de información mayor o igual a 30 días calendario, deben ser inactivadas. La responsabilidad de este control es del Grupo Gestión de Accesos de la Gerencia de Tecnologías de la Información.
e) Todas las cuentas de usuario que lleven deshabilitadas más de 180 días deben ser eliminadas, manteniendo la respectiva trazabilidad y registro. La responsabilidad de este control es del Grupo Gestión de Accesos de la Gerencia de Tecnologías de la Información.
f) Si se identifican cuentas activas de usuarios retirados de la compañía, estas se deben inactivar y eliminar inmediatamente cuando la aplicación lo permita; se debe reportar esta situación como un evento de riesgo de acuerdo con lo establecido en el Sistema Integral de Administración de Riesgos.

Cualquier inconsistencia encontrada en la revisión periódica de los accesos, debe ser reportada como evento de riesgo y ser gestionada como un incidente de Seguridad de la Información.

4.1.9 Gestión de usuarios privilegiados

La gestión de usuarios privilegiados definido por COLPENSIONES, aplica el procedimiento de Gestión de Accesos, el cual debe considerar el cumplimiento de las siguientes políticas:

a) Los privilegios de administrador en los sistemas de información y aplicaciones, así como el acceso remoto para dar soporte a los usuarios, deben estar restringidos únicamente a los colaboradores que lo requieren para el cumplimiento de sus funciones contractuales o laborales.
b) Las cuentas privilegiadas del sistema, las cuales incluyen: administrador, root, sysadmin y admin, no pueden ser usadas de forma directa; en caso de requerir utilizar sus funciones, deberán ser invocadas por medio de la cuenta asignada a un colaborador, quien será responsable de las acciones que se ejecuten.
c) Los usuarios privilegiados deben ser asignados estrictamente a los colaboradores que por su rol lo requieran; se debe garantizar la individualización y trazabilidad de todas las acciones realizadas por cada uno de los usuarios.
d) Todo sistema de información y aplicación debe tener al menos un usuario privilegiado debe contar con un segundo factor de autenticación; su custodia será responsabilidad del propietario del sistema de información o aplicaciones propias de COLPENSIONES.
e) Los sistemas de control de accesos deben dejar registro de todas las actividades realizadas por los usuarios privilegiados, los cuales deben ser monitoreados por la Gerencia de Prevención del Fraude.

4.1.10 Usuarios de servicio

Un usuario de servicio es aquel que utiliza una aplicación para autenticarse sobre otra aplicación o sistema de información; para estos casos se definen los siguientes lineamientos:

a) La creación de usuarios de servicio se permite en COLPENSIONES en los siguientes casos:

- Cuando existen aplicaciones o servicios que requieren utilizar autenticación para la ejecución de procesos o tareas automáticas sin intervención humana.

- Cuando un sistema de control, monitoreo o seguridad, requiere autenticarse en otros componentes para su funcionamiento.

b) Todo usuario de servicio debe ser asignado a un colaborador, el cual es responsable por todas las acciones que se ejecuten por parte de este usuario siguiendo el LINEAMIENTO - CREACIÓN USUARIOS Y CONTRASEÑAS GGT-PSE-LIN-002.
c) La custodia de las credenciales de autenticación de un usuario de servicio debe estar a cargo del colaborador al cual está asignado este usuario.
d) Las contraseñas de los usuarios de servicio deben estar cifradas con un algoritmo de cifrado fuerte; nunca podrán estar en texto plano, restricción que incluye archivos de configuración y código fuente de aplicaciones.
e) Siempre que se requiera almacenar una contraseña, esta deberá ser de forma cifrada con un algoritmo de cifrado fuerte.
f) Los usuarios de servicio no pueden tener privilegios de configuración sobre sistemas operativos, bases de datos y aplicaciones.

4.2 Política de Seguridad de la Información para las relaciones con proveedores

COLPENSIONES mantiene mecanismos de control de cumplimiento de las consideraciones contractuales con terceros, de tal forma que se proteja la información de la Entidad a la que estos tengan acceso y que sea requerida por ellos, para la prestación de sus servicios. Por lo anterior COLPENSIONES divulga y exige el cumplimiento de las políticas y procedimientos de seguridad de la información de la Entidad.

4.2.1 Etapa precontractual

La política establece los siguientes puntos, en las fases previas a la formalización del acuerdo contractual:

a) Durante la etapa precontractual, desde la construcción de los estudios previos, el área solicitante de la contratación debe identificar los riesgos de Seguridad de la Información y ciberseguridad, los cuales deben ser parte de la estimación y cobertura de los riesgos del proceso de contratación. Por la razón anterior, todo contrato con un tercero debe contar con un análisis de riesgos de Seguridad de la Información y ciberseguridad, con el respectivo plan de tratamiento para los riesgos identificados, de acuerdo con la Metodología de Gestión de Riesgos de Seguridad de la Información definida por

COLPENSIONES. Los contratos deben incluir las cláusulas necesarias para asegurar la implementación de los controles que den tratamiento a los riesgos identificados.

b) El líder de proceso o proyecto del contrato debe identificar los activos de información a los cuales debe tener acceso el tercero en el desarrollo del servicio a proveer; debe gestionar con el propietario de la información la autorización para el acceso a esos activos y garantizar el cumplimiento de las condiciones de uso aceptable de acuerdo con la definición del propietario de la información. El cumplimiento de las condiciones de uso aceptable de los activos de información debe quedar explícitamente expresado en el contrato y asegurado por parte del supervisor en el desarrollo del mismo.

c) Se deben generar Acuerdos de Niveles de Servicio (ANS), Acuerdos de Confidencialidad, y/o Acuerdos de Intercambio de Información con todos los terceros que generen una relación contractual con COLPENSIONES. Estos acuerdos deben contener una responsabilidad civil y penal para terceros.

d) El equipo estructurado debe asegurar la inclusión en el contrato de las cláusulas definidas por COLPENSIONES sobre confidencialidad, protección de datos, intercambio de información, derechos de propiedad intelectual, cumplimiento de las políticas de seguridad y privacidad de la información y derechos de autor.

e) El equipo estructurador debe socializar a los proveedores las políticas y procedimientos de Seguridad de la Información y ciberseguridad de COLPENSIONES; la obligación de su cumplimiento debe quedar explícitamente estipulada en el contrato.

f) Para la contratación de servicios o componentes de la infraestructura de TI y/o áreas seguras, se debe exigir a los proveedores la presentación de los planes de contingencia que aseguren la disponibilidad de la información, suministrada y procesada entre las partes, los cuales deben ser resultado de un análisis de riesgos de Seguridad de la Información.

La Gerencia de Tecnologías de la información y la Gerencia de Prevención del Fraude deben asegurar que:

a) La información clasificada y reservada que se transmita desde y hacia terceros, sea cifrada utilizando un algoritmo fuerte de cifrado.
b) Los dispositivos de terceros que se conectan a la red de datos de COLPENSIONES, cuenten con herramientas antimalware actualizadas.

c) Se restringe el acceso de los computadores y dispositivos móviles de terceros que se conectan a la red de datos de COLPENSIONES, exclusivamente a la información autorizada.
d) Se implementan los controles de tecnología requeridos, de acuerdo con el análisis de riesgos realizado para la implementación del servicio objeto del contrato.
e) Verificar el cumplimiento de los controles de software base instalado y de licenciamiento de software, y hacer extensivos los controles existentes en la red a equipos de cómputo de terceras partes, cuando los proveedores que por necesidades o por acuerdos contractuales de la operación, incorporen equipos de cómputo a la red corporativa.

4.2.2 Etapa contractual

Los siguientes son los lineamientos que se deben aplicar durante la ejecución del contrato por parte del supervisor del contrato:

a) Verificar de manera permanente, el cumplimiento de los requisitos de Seguridad de la Información y ciberseguridad establecidos.
b) Monitorear periódicamente el cumplimiento de los Acuerdos de Confidencialidad, Acuerdos de Niveles de Servicio y Acuerdos de Intercambio de información de los proveedores de servicios.
c) El supervisor debe realizar monitoreo sobre el acceso a la información y a los recursos de almacenamiento y procesamiento de ésta por parte de los terceros, para asegurar que se cumplen las condiciones establecidas en el contrato; en caso de presentarse un incidente de Seguridad de la Información, el supervisor debe asegurar que se realice el reporte de acuerdo con el Procedimiento de Gestión de Incidentes de COLPENSIONES definido en el proceso Gestión Integral de Riesgos con código AG-GIR-CAP-001 .
d) El supervisor del contrato debe asegurar que se realicen procesos de auditoría al proveedor, cuyo objetivo sea validar el cumplimiento de los requisitos de Seguridad de la Información y Ciberseguridad definidos en el contrato y consignarlos en los informes de supervisión.
e) Toda gestión del proveedor que represente una modificación, mantenimiento, revisión sobre los servicios de tecnología de la información, comunicaciones o equipos de suministros, debe contar con un análisis de riesgos de Seguridad de la Información y pasar por un Procedimiento de Gestión de Cambios antes de su ejecución.
f) En la relación contractual con proveedores, se debe establecer y monitorear el cumplimiento de las condiciones de seguridad física y del entorno en las instalaciones de procesamiento de información de estos terceros.

g) Los riesgos de Seguridad de la Información relacionados con los proveedores de servicios y/o contratistas, deben ser monitoreados constantemente por el Responsable del Riesgo (Ver documento Roles y Responsabilidades de Seguridad de la Información) durante la vigencia de la relación contractual del tercero.
h) Los accesos a la información de la Entidad requeridos por terceros, deben ser evaluados y aprobados de manera formal acorde con el Procedimiento GESTIÓN DE ACCESOS GGT-PSE-CPR-001.

Los proveedores y contratistas de COLPENSIONES deben:

a) Incluir la gestión de vulnerabilidades de las plataformas que estén bajo su responsabilidad. Esto incluye el reporte oportuno a COLPENSIONES de las vulnerabilidades identificadas y las medidas a implementar para mitigar los riesgos asociados, mientras se generan los parches o actualizaciones requeridos.
b) El proveedor debe entregar a COLPENSIONES la documentación de los procesos y procedimientos con los registros correspondientes, donde se demuestre el cumplimiento de las políticas de Seguridad de la Información en toda la cadena que involucren los servicios contratados.
c) El proveedor debe entregar las herramientas para que COLPENSIONES pueda hacer un seguimiento permanente de las actividades ejecutadas dentro del contrato y con la capacidad de verificar el cumplimiento de los Acuerdos de Niveles de Servicio (ANS) para confidencialidad, integridad y disponibilidad de los activos de información involucrados en el contrato.
d) Utilizar mecanismos criptográficos para el cifrado de la información pública clasificada y pública reservada que sea entregada por COLPENSIONES, acorde a la Política de Uso de Controles Criptográficos y al LINEAMIENTO CONTROLES CRIPTOGRÁFICOS GGT-PSE-LIN-008.
e) Portar la identificación corporativa a la cual pertenece el contratista, durante su permanencia en las instalaciones de la Entidad.

4.2.3 Etapa post contractual

Una vez finalizado el contrato, se deben observar los siguientes aspectos:

a) Durante la etapa post contractual, es función del supervisor del contrato, monitorear y hacer seguimiento a los controles definidos para asegurar la confidencialidad, integridad y disponibilidad de la información, frente a los riesgos previamente identificados ver proceso Gestión Contractual código GAO-GCO-CAP-001

b) El supervisor del contrato debe validar que los controles de Seguridad de la Información y Ciberseguridad definidos a partir del análisis de riesgos, se encuentren debidamente implementados y monitoreados al terminar el contrato.

4.3 Política Seguridad de la Información en los recursos humanos

COLPENSIONES, consciente de la importancia de las personas como factor fundamental dentro del Sistema de Gestión de Seguridad de la Información, establece los siguientes lineamientos para fortalecer la seguridad de la información, al ser los colaboradores quienes interactúan de forma permanente con ella.

a) Al proveerse un nuevo cargo, se debe actualizar la matriz de roles empresariales, adicionando el nuevo rol, los atributos y los privilegios en las aplicaciones o sistemas de información.
b) Todos los trabajadores oficiales, trabajadores en misión, personal SENA y terceros que presten sus servicios a COLPENSIONES y terceros, a los que se brinde información reservada o clasificada, deben firmar como parte de sus términos y condiciones iniciales de trabajo, un Acuerdo de confidencialidad y no divulgación.
c) Este acuerdo debe incluir la aceptación del Manual de políticas y lineamientos en seguridad y privacidad de la información y ciberseguridad, el tratamiento de la información de la Entidad, en los términos de la Ley 1581 de 2012, 1712 de 2014 y las demás normas que la adicionen, modifiquen, reglamenten o complementen. Este documento debe ser conservado por la Gerencia de Talento Humano.
d) Se debe contar con un programa de capacitación y sensibilización en Seguridad de la Información, el cual debe contemplar en su contenido: políticas y procedimientos, roles y responsabilidades, metodología de activos, metodología de riesgos, marco legal y regulatorio de Seguridad de la Información.
e) Todo colaborador debe recibir una inducción sobre las políticas y procedimientos de Seguridad de la Información al iniciar su relación contractual con COLPENSIONES.
f) El proceso de contratación de personal debe incluir la verificación de antecedentes disciplinarios y estudio de seguridad del candidato. Esto aplica para todos los trabajadores oficiales asociados al Procedimiento de Selección CÓDIGO. GTH-GSA-CAP-001.
g) Todos los colaboradores de COLPENSIONES deben cumplir las políticas de Seguridad de la Información de la Entidad; esta obligación debe estar estipulada de forma explícita en el contrato.

h) Es responsabilidad del Gerente del Área o Supervisores de Contrato, registrar a través de la herramienta tecnológica dispuesta para tal fin, las novedades de los colaboradores de su área tales como: retiros, vacaciones, cambio de área entre otros, asociadas con su relación contractual con COLPENSIONES, especificando la fecha en la cual se hará efectiva.
i) La Gerencia de Talento Humano debe tramitar a través de la herramienta tecnológica dispuesta para tal fin, todas las novedades relacionadas con los colaboradores de COLPENSIONES tan pronto éstas sean notificadas; las novedades comprenden: vinculación, desvinculación, reubicación, traslado, cambio de dependencia, cambio de cargo, licencia, vacaciones, permiso o incapacidad.
j) Un incumplimiento a las políticas de Seguridad de la Información y ciberseguridad de COLPENSIONES, constituye un incidente de Seguridad de la Información, el cual debe ser reportado de acuerdo con el Instructivo Gestión de Incidentes de Seguridad de la Información y ciberseguridad asignado al proceso Gestión Integral de Riesgos AGE-GRI-INS-002, para que surta el análisis respectivo.
k) Todos los colaboradores de COLPENSIONES deben cumplir con un proceso de selección acorde con la criticidad de la información que van a manejar.

4.4 Política de gestión de activos de información

COLPENSIONES debe identificar y clasificar los activos de información.

4.4.1 Consideraciones generales

A continuación, se abordan los lineamientos a aplicar para la gestión de activos de información:

a) Todo activo de información de COLPENSIONES es de uso exclusivo de la Entidad y será utilizado únicamente para su propósito específico.
b) Los activos de información de COLPENSIONES deben ser identificados, clasificados, valorados y marcados de acuerdo con la metodología de identificación, clasificación y valoración de activos de información.
c) Todos los activos de información deben tener un propietario, quien es el responsable de asegurar que su registro en la Matriz de Activos de Información (MAI) se encuentre actualizado, así como del monitoreo y gestión de los controles designando un custodio responsable de los mismos de acuerdo con la clasificación de cada activo, para asegurar la protección de su integridad, confidencialidad y disponibilidad, durante todo su ciclo de vida (producción, recolección, almacenamiento, procesamiento, comunicación y eliminación).

d) La Matriz de Activos de Información (MAI) debe ser actualizada cada vez que se presente la adición o eliminación de uno o más activos de información; también debe ser actualizada si se presenta un **cambio** en la valoración de la confidencialidad, integridad o disponibilidad de un activo de información, o en uno o más campos de su caracterización. Estas situaciones pueden darse, entre otras, por una modificación en el proceso, subproceso o procedimiento, una nueva regulación, adopción de las mejores prácticas del mercado o internacionales o normativa o la materialización de un incidente de seguridad.

e) Se debe hacer al menos una revisión semestral de las Matrices de Activos de Información (MAI) para validar que se han aplicado las actualizaciones pertinentes.

f) El propietario de la información define qué activos de información se pueden manejar o almacenar en dispositivos móviles.

g) El propietario de la información debe definir los procedimientos para controlar y dejar evidencia del ciclo de vida de cada activo de información estableciendo claramente las actividades y sus responsables para la creación, modificación, eliminación, asignación y devolución de cada activo.

h) La copia o transferencia por cualquier medio (físico o digital) de información reservada o clasificada, debe estar autorizada y controlada por el propietario de la información.

i) El propietario de la información debe monitorear el acceso a los activos de información clasificados y reservados.

j) Todos los activos de información deben ser marcados, independiente del medio en el que se encuentren, identificando el nivel de clasificación frente a la confidencialidad, integridad y disponibilidad establecida en la Matriz de Activos de Información. Las etiquetas se deben poder reconocer fácilmente.

k) La información reservada o clasificada debe estar cifrada para su almacenamiento.

l) El intercambio de información reservada o clasificada en formato digital, se debe realizar de acuerdo con el INSTRUCTIVO PARA LA TRANSFERENCIA DE INFORMACIÓN GGT-PSE-INS-024 y LINEAMIENTOS Y ESTÁNDARES DEL GOBIERNO Y GESTIÓN DE TI GGT-GET-LIN-001. Para la información física, este intercambio se debe hacer a través del servicio de mensajería privada, por medio de paquetes sellados que no permitan observar su contenido.

m) No está permitido el uso de herramientas de colaboración de proveedores de servicios en la nube, como repositorio documental. Dado que por necesidades de los procesos esta herramienta se utiliza para el trabajo colaborativo en la fase de elaboración de documentos, y teniendo en cuenta que de acuerdo con la ley 1712 de 2014 un documento en construcción no puede ser considerado información pública, esta información debe contar con la protección propia de los activos de información clasificados o reservados.

n) La destrucción, extracción, transmisión, copiado y divulgación no autorizada de activos de información de la Entidad, en cualquier medio o formato se considera un incumplimiento de las políticas y por lo tanto, un incidente de seguridad de la información y ciberseguridad.

4.4.2 Modificación directa sobre Base de datos en producción

No está permitido el acceso directo a bases de datos en producción para consulta o modificación, tal como lo establece la Política de Control de Acceso; para los casos excepcionales contemplados en dicha política, se deben cumplir los siguientes lineamientos:

a) El análisis de riesgos de Seguridad de la Información que debe realizarse como requisito para estos casos excepcionales (ver Política de Control de Acceso), es responsabilidad del Propietario de la Información (ver Documento de Roles y Responsabilidades de Seguridad de la Información) y debe realizarse siguiendo la Metodología de Gestión de Riesgos de Seguridad de la Información y Ciberseguridad definida por COLPENSIONES.
b) No está permitida la modificación a través del uso de procedimientos almacenados.
c) En los casos en que se requiera la modificación o inactivación de restricciones propias de la base de datos, se debe garantizar que, una vez terminada la modificación de datos, dichas restricciones quedan activas nuevamente.
d) No es permitido agregar, modificar o eliminar restricciones de manera permanente por este mecanismo; dichos cambios deberán surtir el procedimiento definido por la Gerencia de Tecnologías de la Información para la gestión de cambios y liberaciones.
e) Se debe garantizar que, en todas las modificaciones directas de datos, se aplica el principio de segregación de funciones entre los funcionarios de tecnología que construyen los “scripts” de modificación, las áreas funcionales, los dueños de la información que los validan o prueban y los funcionarios de tecnología que los ejecutan. Estos roles deben pertenecer a áreas de reporte independientes dentro de la Gerencia de Tecnologías de la Información.
f) Toda modificación directa de datos requiere que desde la Dirección de Infraestructura de TI antes de su ejecución, se realice una copia de seguridad de los datos y objetos de bases de datos que van a ser alterados por la modificación, la cual debe ser siempre restaurada desde los medios provistos por el área de Infraestructura en caso de que se identifique daño, mal funcionamiento o interrupción abrupta del script de modificación ejecutado. En los casos en que el cumplimiento de este lineamiento no sea viable, se deberá dejar constancia del análisis de riesgos realizado, de la autorización por parte del

propietario de la información, así como de las acciones y controles a realizar en caso de daño, mal funcionamiento o interrupción abrupta del script de modificación ejecutado.

g) Los propietarios de la información en conjunto con la Gerencia de Tecnologías de la Información, deben realizar el monitoreo pertinente para asegurar la integridad y confidencialidad de los datos previo, durante y posterior a la ejecución del procedimiento de actualización.
h) Todas las acciones realizadas sobre la base de datos, deben quedar debidamente registradas en los logs de eventos respectivos, de manera que se cuente con la trazabilidad de toda la actividad desarrollada.
i) No se permite la construcción, modificación o eliminación de restricciones técnicas que hayan sido previamente parametrizadas, índices, procedimientos almacenados, tablas, vistas u otros elementos de bases de datos permanentes, por lo que cualquier elemento que se cree para realizar la modificación debe ser eliminado una vez termine la ejecución del script. El incumplimiento de esta política es clasificado como una violación disciplinaria y se informará a la Oficina de Control Interno Disciplinario para su respectivo trámite.

4.5 Política de uso aceptable de activos de información

Es responsabilidad del propietario del activo de información, la definición de las reglas sobre la forma cómo se restringe o permite el uso de la información en conjunto con el custodio definiendo los controles técnicos; esto determina:

a) Dónde puede ser almacenado.
b) Si puede o no ser impreso.
c) En caso de ser un documento impreso, si puede o no salir de las instalaciones de la Entidad.
d) Si se puede o no transferir.
e) Si se puede procesar o almacenar en la nube.
f) Si se debe firmar digitalmente.
g) El registro de su uso.
h) Si se debe cifrar.
i) Los privilegios para todo su ciclo de vida.
j) En qué casos habría excepciones para las definiciones anteriores.

4.6 Política seguridad física y ambiental

Se debe prevenir el acceso físico no autorizado, para tal fin, la Dirección de Bienes y Servicios y el propietario del activo de información deben:

a) Establecer controles de acceso para las áreas seguras y de acceso restringido de COLPENSIONES (centros de procesamiento principal y alterno, centros de comunicaciones, centros de cableado principal, áreas definidas para dispositivos de almacenamiento de información, áreas donde se procesen dineros, información y títulos valor, áreas donde se deposite salidas de impresoras o fax); como, por ejemplo: puertas de seguridad, sistemas de control con lectores biométricos, cámaras de vigilancia, sistema de alarmas, archivadores bajo llave, entre otras, que el análisis de riesgos y su plan de tratamiento determine necesarios.
b) Señalizar las áreas de acceso restringido, previamente identificadas por los procesos y concertadas con las áreas.
c) Asegurar el monitoreo por CCTV (Circuito cerrado de televisión) a las áreas seguras y de acceso restringido, asegurando que las cámaras no apunten directamente a la captura de información dentro de estas áreas.
d) Las oficinas vacías deben estar aseguradas con llave de manera permanente.
e) Realizar las adecuaciones físicas necesarias (instalación de muros, vallas, alarmas, suelos, protección de ventanas, torniquetes de acceso, cerraduras, espejos de vigilancia o seguridad etc.) para la protección del perímetro de las instalaciones donde se almacena o procesa información, de acuerdo con el análisis de riesgos.
f) Implementar los controles necesarios para la protección del cableado eléctrico y de datos en las instalaciones de la Entidad, contra daños físicos y manipulación.

4.6.1. Trabajo en áreas seguras

Las áreas deben contar con protecciones físicas y ambientales, acordes con el valor y la necesidad de aseguramiento de los activos que se protegen, de acuerdo con el análisis de riesgos realizado por el propietario del activo de información.

a) La Gerencia Administrativa, será responsable de controlar el ingreso y salida del personal a las áreas seguras y de acceso restringido según los accesos definidos por el propietario de la información.
b) Se debe restringir el uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles.

c) No se permite el uso de celulares en áreas seguras y de acceso restringido
d) La Gerencia Administrativa debe señalizar de forma gráfica las restricciones para que estas se visualicen antes del ingreso.
e) El trabajo en áreas seguras y de acceso restringido debe estar monitoreado por CCTV, teniendo en cuenta que las cámaras no podrán apuntar directamente a la captura de información dentro de estas áreas.
f) Todo el personal que ingrese a las áreas seguras y de acceso restringido debe portar identificación visible y presentarla al personal de vigilancia en la puerta de acceso antes de su ingreso, siendo registrados en las minutas de control de acceso.
g) El ingreso se debe hacer con acompañamiento de un servidor público de la dependencia responsable del área segura o de acceso restringido.
h) Se debe asegurar que los centros de cableado se encuentran separados de áreas que contengan líquidos inflamables o propensas a inundaciones o incendios, de acuerdo con el concepto de un especialista en esta materia.
i) La Gerencia de Tecnologías de la Información es responsable por el mantenimiento de la infraestructura física de los centros de cableado a nivel nacional, la cual incluye puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, entre otros.
j) La Gerencia de Tecnologías de la información debe realizar una revisión periódica del estado de los centros de cableado y gestionar la reparación inmediata de las anomalías que identifique, las cuales incluyen: daños en racks, en equipos activos de red y en infraestructura física (puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, entre otros).
k) Se debe establecer un plan de mantenimiento para los centros de cableado por parte de la Gerencia de Tecnologías de la Información, mediante los cuales se corrijan las fallas evidenciadas y se identifiquen puntos de mejora.
l) Los videos de las cámaras de vigilancia están bajo custodia de la Gerencia Administrativa, deben estar registrados en la MAI del proceso respectivo y contar con los controles que aseguren su disponibilidad e integridad.
m) La Gerencia de Tecnologías de la Información debe mantener las áreas relacionadas con procesamiento de información libres de objetos y elementos que no sean propios de la operación.
n) Las áreas relacionadas con procesamiento de información deben contar con control de programación de mantenimientos preventivos, teniendo en cuenta los niveles de servicio acordados con los responsables de la prestación de estos servicios y los cronogramas establecidos por la Gerencia de Tecnologías de la Información.

o) La Gerencia de Tecnologías de la Información debe asegurar la ejecución periódica de mantenimientos preventivos y pruebas de funcionalidad de los sistemas de UPS, plantas eléctricas, detección de incendios y aire acondicionado.
p) Se deben implementar los controles para asegurar el suministro eléctrico para los equipos de TI de acuerdo con el resultado de los análisis de riesgos de Seguridad de la Información.
q) Los responsables de la custodia de las áreas relacionadas con procesamiento de información, deben asegurar que se cumplen las condiciones ambientales requeridas.
r) La Gerencia Administrativa debe realizar campañas de socialización y concienciación acerca de los controles físicos, la política de acceso a las instalaciones y las actualizaciones que se presenten sobre ellos.
s) La Gerencia de Tecnologías de la Información debe:

- Conservar y mantener actualizados los planos del cableado de las instalaciones de COLPENSIONES
- Conservar y mantener actualizada la Topología de Red de COLPENSIONES
- Mantener los cables de red y en general todos los dispositivos de los centros de datos claramente marcados.
- Controlar el acceso a los centros de cableado sólo para el personal autorizado.

4.6.2 Controles físicos de ingreso a las instalaciones y a las áreas restringidas

Se deben implementar controles de acceso físico a las diferentes instalaciones de COLPENSIONES:

a) Se debe validar la identificación de todas las personas que ingresen a las instalaciones de COLPENSIONES; su ingreso se debe hacer de forma individual.
b) Para el acceso físico a las instalaciones de la Entidad, debe seguirse el Instructivo Seguridad Física y Control de Acceso GAO-GBS-INS-004.
c) Todos los colaboradores de COLPENSIONES deben portar el carné en un lugar visible mientras se encuentren en las instalaciones de la Entidad.
d) Los Visitantes que ingresan a la Entidad deben tener un carné o distintivo de visitantes que los identifique, en un lugar visible dentro de las instalaciones de la Entidad.
e) Los colaboradores deben permitir la verificación de bolsos, maletas o paquetes que ingresen o salgan de las instalaciones de la Entidad, sin excepción.

f) Los colaboradores de la Entidad no deben intentar ingresar a las áreas a las cuales no tengan autorización salvo por alguna excepción que defina la alta Gerencia de la Entidad, o una situación de emergencia que lo obligue.
g) El personal de vigilancia debe estar capacitado y entrenado para aplicar los controles de acceso físico y lógico de la Entidad.

4.7 Política seguridad de las operaciones

Se definen los siguientes lineamientos orientados a asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

a) Los procedimientos para las actividades operacionales asociadas con las instalaciones de procesamiento y comunicación se deben documentar y poner a disposición de los colaboradores.
b) La Gerencia de Tecnologías de la Información debe gestionar la capacidad de los sistemas de procesamiento de información y comunicaciones, lo cual comprende:

- Evaluar los requisitos de capacidad teniendo en cuenta la criticidad para el negocio.
- Realizar el dimensionamiento a partir de los requerimientos de los sistemas en operación y proyectar las futuras demandas.
- Monitorear el rendimiento de la infraestructura tecnológica para determinar el uso de la capacidad existente.
- Documentar los datos de rendimiento y capacidad de la plataforma tecnológica de COLPENSIONES.
- Documentar los acuerdos de niveles de servicio.
- Implementar las soluciones de hardware y software, de acuerdo con el dimensionamiento realizado.
- Definir umbrales sobre las variables asociadas a la capacidad (procesamiento, almacenamiento, ancho de banda, entre otras), para tomar decisiones oportunas en caso de ser alcanzados.
- Asignar un responsable de la Gestión de Capacidad.

c) La Gerencia de Tecnologías de la Información debe asegurar que todos los sistemas cuenten con sincronización de reloj a nivel de sistema operativo, teniendo como referencia la hora legal colombiana. No está permitida la desactivación del sistema de sincronización o la manipulación de la hora.

d) La Gerencia de Tecnologías de la Información debe generar y mantener registros de auditoría sobre las actividades de los usuarios, excepciones y eventos de Seguridad de Información. Ver
e) Los registros de auditoría deben contar con controles para garantizar su integridad.
f) La Gerencia de Tecnologías de la Información debe asegurar que las reglas de los firewalls y las firmas de los IPS/IDS, están configuradas de acuerdo con la lógica de negocio de los sistemas de información y aplicaciones de COLPENSIONES; se debe garantizar que esta configuración permanece actualizada y se encuentra debidamente documentada. Ver instructivo Gestión de eventos de riesgos. COD. AGE-GIR-INS-001.
g) Se debe realizar una revisión semestral de la configuración de los dispositivos de seguridad perimetral. Deben habilitarse sólo los servicios y protocolos necesarios según lo requiera el negocio.
h) Los procedimientos operacionales deben asegurar el principio de segregación de funciones, con base en los análisis de riesgos de Seguridad de la Información.

4.8 Política de seguridad en las comunicaciones digitales

Las comunicaciones digitales corresponden a las diferentes formas de transferencia de información a través de medios electrónicos, los cuales incluyen: correo electrónico, mensajería instantánea, redes sociales y herramientas colaborativas.

a) El propietario de la información debe definir dentro del uso aceptable, la forma en que es permitida la comunicación digital, señalando cuando sea necesario, el uso de controles criptográficos para proteger la confidencialidad y la integridad.
b) Se debe implementar la trazabilidad de las comunicaciones digitales, garantizando las evidencias necesarias para la gestión de incidentes, auditorías o solicitudes de entes de control.
c) El uso de las comunicaciones digitales debe estar plenamente justificado por las labores asignadas al cargo del responsable correspondiente. La validación de los contenidos que incumplan esta política es una actividad de la Gerencia de Tecnologías de la Información, la evaluación y medidas correspondientes son responsabilidad de la Gerencia de Talento Humano.
d) El intercambio de información por este medio debe estar estrictamente ajustado al origen y destino autorizado, asegurando que se mantengan las condiciones de seguridad en todo momento y se cumpla lo que establezca la política de control de acceso de la información involucrada.
e) Se debe guardar el registro digital de las comunicaciones digitales, de acuerdo con lo establecido en el Marco Legal y Regulatorio Colombiano.
f) No se debe guardar un registro impreso de las comunicaciones digitales, ni se debe realizar descargas en equipos personales o de terceros de la información de COLPENSIONES.

g) Cualquier tipo de comunicación digital debe ser firmada por el colaborador que la origina.
h) Los usuarios son responsables de la validación del contenido de los mensajes recibidos y deben abstenerse de la ejecución o uso de los archivos adjuntos, cuando no cumplan con las políticas de Seguridad de la Información.
i) Las comunicaciones digitales pueden ser objeto de monitoreo por efectos de gestión de riesgos de Seguridad de la Información.
j) Los servicios de comunicaciones digitales (correo electrónico, mensajería instantánea, redes sociales, herramientas colaborativas), deben ser utilizados con cuentas de usuario asignadas en forma personal e intransferible a cada colaborador.
k) Cuando se requiera el uso compartido de una cuenta, se deberá implementar un mecanismo que enmascare con un nombre identificativo común (Modelo de Seguridad y Privacidad de la Información, Gestión SI), manteniendo la trazabilidad de los colaboradores en forma independiente. En ningún caso se acepta compartir cuentas de usuario por dos o más colaboradores.
l) Los mensajes y la información contenida en los buzones de correo son de propiedad de COLPENSIONES.
m) Cada colaborador se hace responsable del manejo del software cliente asignado (buzón de correo, cliente de mensajería instantánea, software para herramientas colaborativas) para el servicio de comunicaciones correspondiente.
n) Las comunicaciones digitales para asuntos personales, deben estar autorizadas por el jefe Inmediato posterior al respectivo análisis de riesgos.
o) La información clasificada en los niveles de confidencialidad alto y medio, sólo puede ser almacenada en forma cifrada, en servidores de almacenamiento autorizados por el propietario y que cumplan con la política de control de acceso correspondiente.
p) El intercambio de información por medios digitales debe realizarse de acuerdo con el Procedimiento *Transferencia de Información*, enviar mensajes a quienes lo requieren recibir y evitar la copia innecesaria a otros usuarios
q) El envío de la información reservada o clasificada desde cuentas personales está prohibido, así como el reenvío de dicha información a cuentas de correo electrónico externo. No está permitido que los usuarios del servicio de correo electrónico corporativo reenvíen o configuren la redirección automática de los mensajes hacia cuentas de correo electrónico externas.

4.9 Política para adquisición, desarrollo y mantenimiento de sistemas de información

El software se constituye en una herramienta de trabajo muy importante para COLPENSIONES, por lo cual su uso se debe hacer de acuerdo con los siguientes lineamientos:

a) La Gerencia de Tecnologías de la Información es la responsable de planificar, desarrollar y ejecutar las actividades relacionadas con desarrollos, actualizaciones e instalaciones de software. Debe planificar la ejecución de pruebas funcionales y de seguridad de los sistemas nuevos o modificados antes de la instalación en los entornos de producción.
b) El responsable del software que son los propietarios del activo de información y todos los colaboradores del área independiente de su nivel de autoridad que deben realizar un análisis de riesgos de Seguridad de la Información en la fase inicial del ciclo de desarrollo, a partir del cual se debe realizar la especificación de los requerimientos de seguridad, tanto para desarrollos internos como para el software adquirido.
c) Se debe asegurar que la información se realice a través de algoritmos fuertes de cifrado acorde al LINEAMIENTO CONTROLES CRIPTOGRÁFICOS GGT-PSE-LIN-008.
d) Todo desarrollo y actualización de software debe cumplir con el procedimiento de gestión de cambios previo a la puesta en producción.
e) Se deben realizar pruebas mediante las cuales se asegure que los controles de Seguridad de la Información fueron implementados de acuerdo con los requerimientos; los resultados deben ser documentados.
f) La Gerencia de Tecnologías de la Información debe implementar controles de restricción sobre los Sistemas Operativos, para evitar que los usuarios no autorizados puedan instalar software.
g) La Gerencia de Tecnologías de la Información debe autorizar la instalación de todo el software que sea utilizado en COLPENSIONES.
h) La Gerencia de Tecnologías de la Información debe aplicar los controles necesarios para garantizar la integridad y confidencialidad del software de instalación, de paquetes, aplicaciones o sistemas operativos que la Entidad haya descontinuado.
i) La Gerencia de Tecnologías de la Información debe garantizar que las aplicaciones de software utilizadas en COLPENSIONES se encuentren actualizadas y soportadas; debe asegurar la instalación de los parches de seguridad establecidos por el proveedor.
j) El periodo de conservación de dicha información debe definirse de acuerdo con la necesidad de COLPENSIONES para el cumplimiento legal y regulatorio, así como las necesidades del negocio, para recuperar o acceder a información ligada a versiones anteriores de programas.
k) Cuando se determine la eliminación definitiva del software en desuso o descontinuado, este deberá ser destruido físicamente si se encuentra en CD, DVD, cintas u otros medios o borrados de manera segura para que no se pueda recuperar la información.

l) Se debe definir una estrategia de retorno (rollback) como requisito para la autorización e implementación de cambios.
m) Las versiones previas del software de aplicación se deben retener como una medida de contingencia.
n) Se debe garantizar que la versión del software usado en sistemas en producción cuente con soporte por parte del proveedor.
o) Los desarrollos de software internos o externos deben cumplir con las políticas de Desarrollo Seguro y Gestión de Vulnerabilidades.
p) COLPENSIONES debe realizar auditorías a terceros para asegurar que se cumplen las políticas de Seguridad de la Información de la Entidad.

4.10 Política de gestión de incidentes de Seguridad de la Información

Se debe garantizar que cualquier evento que pueda afectar la integridad, confidencialidad o disponibilidad de la información, sea identificado oportunamente, reportado y tratado de acuerdo con la criticidad que pueda representar para COLPENSIONES, de tal manera que se evite o se minimice los daños para la Entidad y que haya un aprendizaje para que se prevenga su recurrencia.

4.10.1 Obligación de reporte y gestión

El éxito de la gestión de incidentes depende de muchos factores; uno de ellos es el compromiso de los colaboradores con el reporte de eventos:

a) Para la gestión de incidentes se debe seguir paso a paso el Instructivo Gestión de incidentes de Seguridad de la Información y ciberseguridad, AGE-GRI-INS-002, del proceso Gestión Integral de Riesgos. Los colaboradores deben reportar los eventos de Seguridad de la Información utilizando este procedimiento.
b) Se considera un evento de Seguridad de la Información, cualquier situación relacionada con el incumplimiento de las políticas o procedimientos de Seguridad de la Información.
c) Es obligación de todo colaborador reportar todo evento que pueda comprometer la Seguridad de la Información siguiendo el Instructivo de Gestión de Incidentes de Seguridad y ciberseguridad AGE-GRI-INS-002, del proceso Gestión Integral de Riesgos.
d) La Gerencia de Riesgos y Seguridad de la Información debe:

- Definir, implementar, analizar y mejorar el proceso definido para gestionar los incidentes de Seguridad de la Información y ciberseguridad, de acuerdo con las buenas prácticas de industria y con la legislación aplicable vigente.
- Realizar actividades de análisis o retroalimentación post-incidente para aprender de los incidentes de Seguridad de la Información y ciberseguridad y documentar las lecciones aprendidas de manera adecuada.
- Preparar los reportes a la Junta Directiva de la gestión de incidentes de Seguridad de la Información y Ciberseguridad

e) La Gerencia de Riesgos y Seguridad de la Información es responsable por la valoración y escalamiento de todos los incidentes de Seguridad de la Información reportados.

f) El escalamiento debe hacerse al técnico responsable de su tratamiento y al propietario de la información afectada.

g) El registro de los eventos de Seguridad de la Información debe hacerse en el Sistema de Información designado para este propósito y estar soportado por las comunicaciones o el correo electrónico corporativo enviado al colaborador que reportó el incidente, al responsable de su tratamiento y al propietario de la información afectado.

h) El propietario de la información afectado por un incidente es el responsable por el contacto con las autoridades cuando el incidente de seguridad así lo amerite.

i) El propietario de la información debe proceder con la gestión de riesgos de Seguridad de la Información que aplique, una vez se declare un incidente que afecte un activo bajo su responsabilidad.

j) El propietario del activo de información afectado por un incidente es el responsable por la gestión requerida para el proceso de aprendizaje en COLPENSIONES que evite la recurrencia de ese tipo de situaciones. Para esto debe contar con la participación activa de los procesos de soporte que aplique como son: Gobierno y Gestión de Tecnologías de la Información, Gestión del Talento Humano y Gestión de Bienes y Servicios.

k) Es responsabilidad de la Vicepresidencia de Seguridad y Riesgos Empresariales presentar un informe al menos semestral a la Junta Directiva, sobre los incidentes de Seguridad de la Información y

ciberseguridad ocurridos, las actividades de gestión realizadas y las medidas de control implementadas para evitar su recurrencia.

4.10.2 Preparación para la gestión de incidentes

Se deben cumplir los siguientes lineamientos en la preparación de la gestión de incidentes:

a) La Gerencia de Riesgos y Seguridad de la Información debe disponer los recursos necesarios para realizar la adecuada gestión de incidentes de Seguridad de la Información y ciberseguridad, por ejemplo y sin limitarse a ellos, recurso humano capacitado y disponible, estrategias, guías o instructivos de comunicación interna, externa y otras actividades que considere oportunas o necesarias.
b) La Vicepresidencia de Planeación y Tecnologías de la Información debe disponer los recursos necesarios para realizar la adecuada gestión de incidentes de Seguridad de la Información y ciberseguridad, por ejemplo y sin limitarse a ellos, recurso humano capacitado y disponible, herramientas de software y hardware propias o tercerizadas, estrategias, guías o instructivos de comunicación interna, externa y otras actividades que considere oportunas o necesarias.
c) La gestión de incidentes debe integrar los incidentes con origen en TI, personas e infraestructura para que los 3 tipos de incidentes sean manejados por una sola mesa de servicios.
d) Para garantizar una conciencia de Seguridad de la Información y ciberseguridad en la Entidad, la Gerencia de Riesgos y Seguridad de la Información, debe establecer una estrategia de divulgación y capacitación dirigida a todos los colaboradores, incluyendo en ella la aplicación del Procedimiento de Gestión de Incidentes de Seguridad de la Información, la tipificación de los incidentes de Seguridad de la Información y ciberseguridad, los vectores comunes de ataque y las estrategias de prevención.
e) La Gerencia de Riesgos y Seguridad de la Información, debe establecer los equipos especializados, los terceros y los canales de reporte con dichos entes externos con quienes se debe gestionar o a quienes se debe reportar incidentes de Seguridad de la Información y ciberseguridad de acuerdo con criterios internos y en cumplimiento de la legislación aplicable vigente.
f) Con el ánimo de prevenir o reducir la probabilidad de ocurrencia de incidentes de Seguridad de la Información y ciberseguridad, la Gerencia de Riesgos y Seguridad de la Información debe definir estrategias que le permitan tener alertas tempranas y gestionarlas de acuerdo con su aplicabilidad en la Entidad.
g) Sobre cada riesgo identificado, se deben establecer los controles para el monitoreo de las amenazas que puedan causarlo; este resultado se debe integrar al procedimiento de gestión de incidentes.

4.10.3 Equipo de respuesta a incidentes (ERI)

Los siguientes son los lineamientos sobre el Equipo de Respuesta a Incidentes (ERI):

a) Es responsabilidad de la Vicepresidencia de Seguridad y Riesgos empresariales constituir, formalizar y mantener un grupo de colaboradores entrenados en el manejo de incidentes de Seguridad de la Información y ciberseguridad, los cuales conformarán el Equipo de Respuesta a Incidentes (ERI).
b) El ERI debe estar conformado al menos por representantes de la Gerencia de Riesgos y Seguridad de la Información, la Gerencia de Prevención de Fraude y la Gerencia de Tecnologías de la Información.
c) Son responsabilidades del Equipo de Respuesta a incidentes –ERI de acuerdo con el Instructivo Gestión de incidentes de Seguridad de la Información y ciberseguridad, AGE-GRI-INS-002, del proceso Gestión Integral de Riesgos
d) Analizar cada incidente de Seguridad de la Información o ciberseguridad reportado para definir la adecuada gestión, de acuerdo con el *Instructivo para la gestión de incidentes de Seguridad de la Información y ciberseguridad*, AGE-GRI-INS-002, del proceso Gestión Integral de Riesgos:

- Articular a las diferentes áreas que deben participar en la gestión de cada incidente de Seguridad de la Información y ciberseguridad.
- Garantizar que cada incidente es gestionado de acuerdo con el plan establecido, en los tiempos definidos y asegurando la completitud del ciclo de vida de gestión y respuesta a un incidente de seguridad.
- Aportar la información que sea requerida para el reporte de incidentes de Seguridad de la Información y ciberseguridad, la cual incluye la descripción de la gestión, respuesta y lecciones aprendidas.

4.10.4 Clasificación y priorización de incidentes

Para la clasificación y priorización de incidentes se define:

a) Es responsabilidad de la Gerencia de Riesgos y Seguridad de la Información, definir los parámetros de clasificación y priorización, utilizados en la Gestión de Incidentes de Seguridad de la Información y Ciberseguridad, así como los criterios de activación del Equipo de Respuesta a Incidentes (ERI).

4.10.5 Detección automática de eventos de riesgo

Para la detección automática de eventos de riesgo se define:

a) La Gerencia de Riesgos de Seguridad de la Información debe definir estrategias automáticas para el monitoreo y detección de posibles eventos de riesgo que puedan constituir o generar incidentes de Seguridad de la Información y ciberseguridad.

4.10.6 Gestión de incidentes

A continuación, se detallan los lineamientos para la gestión de incidentes:

a) Los criterios para definir si un incidente de Seguridad de la Información debe ser escalado al ERI, son establecidos por la Gerencia de Riesgos y Seguridad de la Información.
b) El ERI debe contactar e involucrar a los colaboradores, áreas o grupos de COLPENSIONES que sea necesario para gestionar un incidente de Seguridad de la Información y ciberseguridad.
c) La estrategia de gestión de incidentes de Seguridad de la Información y ciberseguridad, debe contemplar actividades relacionadas con la prevención, detección, análisis, contención, erradicación, recuperación y reporte.
d) Es responsabilidad de la Gerencia de Riesgos y Seguridad de la Información analizar cada uno de los eventos de riesgo reportados para determinar si se trata de un incidente de Seguridad de la Información y ciberseguridad, y si está originado en una vulnerabilidad en la tecnología, las personas o la infraestructura.

4.10.7 Documentación de la gestión de incidentes

Sobre la documentación de la gestión de incidentes se define:

a) La Gerencia de Riesgos y Seguridad de la Información, debe garantizar que cada incidente esté debidamente documentado con la información detallada del evento reportado, la secuencia de actividades desarrolladas para la contención, recuperación e investigación, y las lecciones aprendidas. La documentación debe almacenarse en una carpeta administrada por la Gerencia de Riesgos y Seguridad de la Información destinada para tal fin.

4.10.8 Uso de evidencia digital

Los siguientes son los lineamientos para el uso de evidencia digital:

a) COLPENSIONES debe definir y garantizar los recursos, propios o a través de terceros, requeridos para levantar, preservar y analizar evidencia digital bajo la normatividad interna y en cumplimiento de la legislación vigente aplicable.
b) En la gestión de un incidente de Seguridad de la Información y ciberseguridad el ERI debe determinar la necesidad y oportunidad de realizar un proceso de levantamiento, preservación y análisis de evidencia digital de acuerdo con el *Instructivo Gestión de incidentes de Seguridad de la Información y ciberseguridad, AGE-GRI-INS-002, del proceso Gestión Integral de Riesgos.*
c) Es responsabilidad de la Gerencia de Tecnologías de Información garantizar la custodia de las evidencias tomadas de los elementos tecnológicos asociadas a cualquier evento que desencadene un incidente de Seguridad de la Información en COLPENSIONES.

4.11 Política continuidad de la Seguridad de la Información

El Sistema de Gestión de Continuidad de Negocio es paralelo e independiente al Sistema de Gestión de Seguridad de la Información; dentro del MSPI- Modelo de Seguridad y Privacidad de la Información - se deben implementar los mecanismos para que los controles definidos para proteger la confidencialidad, integridad y disponibilidad de la información se mantengan cuando se activen las estrategias de continuidad y esto se logra a través de los siguientes lineamientos:

a) Los controles criptográficos para proteger la confidencialidad y la integridad, deben ser implementados en las copias de respaldo y los sistemas redundantes.
b) El registro de acciones y operaciones debe mantenerse bajo las mismas condiciones de los sistemas principales en los sistemas redundantes, que se activen en caso de una contingencia.
c) El control de acceso debe mantener las restricciones y privilegios en los sistemas redundantes y para las copias de respaldo, acorde con lo establecido por el propietario de la información.
d) Dentro de los eventos que pueden ocasionar interrupciones en los procesos del negocio, se deben contemplar incidentes de Seguridad de la Información y ciberseguridad, así como los impactos que sobre la Seguridad de la Información se puedan generar por cada uno de los eventos de continuidad identificados.
e) Se deben incluir las pruebas de continuidad de Seguridad de la Información y ciberseguridad en las pruebas y revisiones periódicas del Plan de Continuidad del Negocio, las cuales deben realizarse al

menos anualmente; se debe verificar el cumplimiento de todos los requisitos y controles de Seguridad de la Información y ciberseguridad establecidos.

4.12 Política cumplimiento de Seguridad de la Información

COLPENSIONES debe asegurar el cumplimiento de las leyes, la normatividad aplicable y los requisitos de Seguridad de la Información y Ciberseguridad en el diseño, uso, operación y la gestión de los sistemas de información de la Entidad.

a) Todos los colaboradores de COLPENSIONES deben conocer y cumplir sus obligaciones frente a Seguridad de la Información de acuerdo con el marco legal y regulatorio colombiano, así como las políticas de Seguridad de la Información de la Entidad.
b) Se debe asegurar que los procesos de la cadena de valor de COLPENSIONES, sus subprocesos y procedimientos están definidos de manera que se dé cumplimiento al marco legal y regulatorio colombiano de Seguridad de la Información y las políticas de Seguridad de la Información de la Entidad.
c) Dentro de la legislación y regulación que debe cumplir COLPENSIONES relacionada con Seguridad de la Información se encuentran:

- Ley 1581 de 2012 y decreto reglamentario 1377 de 2013 para la protección de datos personales.
- Ley 1266 de 2018 ley de Habeas Data
- Ley 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Circular Externa 007 de 2018 de la Superintendencia Financiera de Colombia para la Gestión de la Seguridad de la Información y la Ciberseguridad.
- Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC.
- Circular Básica Jurídica de la SFC.
- Circular 029 de 2019 de la SFC.
- Circular Externa 005 de 2019 de la Superintendencia Financiera de Colombia para el uso de servicios de computación en la nube.
- Directiva Presidencial 03 de 15 de marzo de 2021 - Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- Ley 23 de 1982 sobre derechos de autor.
- Circular Interna PRE-0004 del 09 de marzo de 2021
- Los requerimientos de las leyes para restricción de acceso a la información y la protección de la confidencialidad e integridad de la información.

d) COLPENSIONES debe adelantar las acciones necesarias para la protección de la información y los datos, asegurando la protección contra las conductas estipuladas en la Ley 1273 de 2009, o Ley de Delitos Informáticos.
e) Se debe aplicar la Ley de Protección de Derechos de Autor para todos los documentos y software utilizados por COLPENSIONES. Se debe cumplir con los siguientes aspectos:

Los presentes lineamientos aplican para los documentos impresos y digitales.

- Se deben identificar los derechos de uso de cualquier documento que sea requerido por COLPENSIONES y cumplir estrictamente lo que el autor o titular de los derechos patrimoniales establezca.
- La copia de un documento únicamente puede llevarse a cabo si es un documento público o si se adquirió el derecho para esta acción, teniendo claro que el valor es proporcional al número de copias que se generen.
- Todos los documentos bajo la responsabilidad de COLPENSIONES, deben cumplir con el marcado de activos de información definido en la *Metodología de identificación, clasificación y valoración de activos de información* y así facilitar la identificación de la restricción de acceso que aplique.
- En ninguna circunstancia se puede publicar en cualquier medio, documentos reservados o clasificados, es decir, aquellos clasificados con nivel “Alto” o “Medio” de confidencialidad en las matrices de activos de información.
- Todo el software que se utilice en COLPENSIONES debe estar licenciado, esto es independiente de cualquier condición, es decir, aplica si el software es comercial o gratuito, abierto o cerrado, si es para un servidor o para un computador de usuario, si está en demostración o en uso.
- Se debe tener claro que el licenciamiento de un software no se limita al pago de los derechos patrimoniales sino también a las condiciones de uso y las exigencias que el autor pueda hacer en los términos existentes.
- Todo el software que se adquiera o use en COLPENSIONES debe cumplir con la verificación de los requisitos legislativos y normativos relacionados con los derechos de propiedad intelectual.
- Los Líderes de los procesos deben estimar dentro de sus presupuestos los costos relacionados con el licenciamiento de uso de software y documentos.

4.13 Política dispositivos para movilidad y acceso remoto

Con el fin de dar cumplimiento al tratamiento definido para los activos de información en dispositivos móviles, se deben cumplir las siguientes directrices:

4.13.1 Movilidad

COLPENSIONES reconoce que, por el objeto de su misión, y por su naturaleza y tamaño, cuenta con diferentes sedes entre las cuales están distribuidas sus áreas y servidores públicos; por tal razón define estrategias de movilidad que faciliten el desplazamiento sin afectar la operación.

a) Las estrategias de movilidad definidas, deben garantizar que la información permanece confidencial, íntegra y disponible en niveles acordes con su clasificación.
b) Son catalogados como dispositivos móviles: computadores portátiles, tabletas, terminales livianas y teléfonos móviles; la Gerencia de Tecnologías de la Información debe instalar y configurar los controles de seguridad requeridos según el análisis de riesgos realizado y revisado al menos una vez al año.
c) La Gerencia de Tecnologías de la Información sólo podrá instalar en los dispositivos móviles las aplicaciones definidas y autorizadas, teniendo en cuenta el análisis de riesgos realizado por dicha gerencia.
d) La Gerencia de Tecnologías de la Información debe mantener activas y sin modificación en su configuración, las protecciones de seguridad definidas para dispositivos móviles.
e) En los dispositivos móviles se debe cumplir con la Política de Control de Acceso correspondiente a la información que maneje.
f) El propietario de la información define qué activos se permiten manejar en estos dispositivos.
g) Si es requerido establecer una comunicación de datos desde un dispositivo móvil provisto por Colpensiones con otro dispositivo interno y/o externo, se debe asegurar que la comunicación cuente con mecanismos seguros de interconexión de acuerdo con lo descrito en el LINEAMIENTO DE SEGURIDAD PARA EL ACCESO A REDES INALAMBRICAS CORPORATIVAS GGT-PSE-LIN-004 y GUIA PARA CONFIGURACIÓN DE CONEXIÓN A LA RED INALAMBRICA TERCEROS A COLPENSIONES GGT-GSO-GUI-038 definidos por la Gerencia de Tecnologías de la Información.
h) La conexión remota por parte de los colaboradores sólo se debe hacer a través de la solución de conexión establecida por la Entidad, la cual debe contar con la implementación de los controles definidos a partir del análisis de riesgos de Seguridad de la Información y Ciberseguridad para esta solución realizado por la Gerencia de Tecnologías de la Información, considerando segundo factor de

autenticación, validaciones de seguridad del equipo antes del ingreso, control de origen de conexión (ubicación, equipo).

i) La solución de conexión remota establecida por la Entidad, debe asegurar que no es posible copiar la información hacia el dispositivo desde el cual se está haciendo la conexión.
j) Los equipos desde los que se haga la conexión a COLPENSIONES, deben cumplir las políticas de Seguridad de la Información y Ciberseguridad de la Entidad.

4.13.2 Obligaciones de los usuarios de dispositivos móviles de COLPENSIONES

Es responsabilidad de los usuarios que, de acuerdo con sus funciones y bajo autorización del líder de proceso informando a la Gerencia de Tecnologías de la Información, les sea permitido el uso de dispositivos móviles propios o de COLPENSIONES para el desempeño de sus funciones:

a) Reportar cualquier evento de riesgo que pueda afectar la protección de la información, particularmente cuando su dispositivo ha sido robado o extraviado o se evidencien los accesos no autorizados.
b) Cumplir las políticas y procedimientos de Seguridad de la Información y ciberseguridad de COLPENSIONES.
c) Activar las características de cifrado del dispositivo móvil.
d) Mantener en todo momento el sistema operativo actualizado.
e) No descuidar el dispositivo móvil en ningún momento.
f) Mantener la pantalla bloqueada si no está utilizando dispositivo móvil, activando la opción de desbloqueo por código de acceso, huella o contraseña, de acuerdo con el dispositivo que aplique.
g) Navegar responsablemente por Internet de acuerdo con las políticas y lineamientos de Seguridad de la Información y ciberseguridad del presente manual.
h) No mantener activas las opciones de conexión inalámbrica que no vayan a ser utilizadas.
i) No conectarse a redes Wi-Fi públicas abiertas.
j) Participar en las campañas de concientización sobre temas de riesgos, Seguridad de la Información y ciberseguridad, adelantadas por COLPENSIONES.
k) Asegurar que mientras digita la contraseña en su dispositivo móvil nadie esté observando.
l) Permitir los procesos de actualización de aplicaciones y sistema operativo de acuerdo con los lineamientos de la Gerencia de Tecnologías de la Información.
m) No procesar ni almacenar información clasificada o reservada en el dispositivo móvil.

4.13.3 Dispositivos móviles provistos por COLPENSIONES

Los siguientes son los lineamientos para el uso de dispositivos móviles de COLPENSIONES:

a) Los dispositivos móviles propiedad de COLPENSIONES que puedan llegar a almacenar información de tipo reservada o clasificada, deben contar con controles de borrado o inactivación remota para garantizar que usuarios no autorizados en caso de hurto o pérdida accedan a la información.
b) Es responsabilidad de la Gerencia de Tecnologías de Información instalar y configurar adecuadamente los controles de borrado o inactivación remota.
c) Los dispositivos móviles propiedad de COLPENSIONES, deben tener controles de acceso que garanticen la identificación de los usuarios y limiten el acceso a la información en ellos contenidos de acuerdo con su perfil.
d) Los dispositivos móviles propiedad de COLPENSIONES deben estar configurados por la Gerencia de Tecnologías de Información para bloquearse automáticamente después de tres (03) minutos de inactividad.
e) Los dispositivos móviles propiedad de COLPENSIONES, que soporten la funcionalidad, deben mantener la geolocalización activada para permitir su rastreo remoto, a través del sistema de posicionamiento global (GPS por sus siglas en inglés), en caso de pérdida o hurto.
f) Los dispositivos móviles propiedad de COLPENSIONES deben mantenerse con las opciones de conectividad Wifi, Bluetooth, NFC y otras tecnologías de conexión remota apagadas. Únicamente deberán encenderse cuando sea estrictamente necesario.
g) Los dispositivos móviles propiedad de COLPENSIONES deben tener instaladas las herramientas antimalware definidas por la Gerencia de Tecnologías de Información; se debe asegurar que se realicen las actualizaciones de firmas con la periodicidad establecida por la Entidad.
h) El software antimalware debe estar configurado para que se actualice automáticamente sin intervención de los usuarios finales.
i) El software antimalware debe estar configurado para realizar análisis periódicos y remediación sin intervención de los usuarios finales.
j) El software antimalware no podrá ser desactivado, desinstalado o inhabilitado por los usuarios finales.
k) El software antimalware debe cumplir con las Políticas contra Código Malicioso definidas por la Gerencia de Riesgos y Seguridad de la Información.
l) La instalación de software en dispositivos móviles debe seguir los lineamientos establecidos en la Política para el licenciamiento y uso de software.

m) Los dispositivos móviles propiedad de COLPENSIONES que lo permitan deben contar con controles para restringir el tráfico de información entrante y saliente, así como tener software de propósito específico para garantizar que se mantengan las políticas de navegación en internet y no se acceda a páginas web con contenido explícitamente prohibido. Dichos controles no deben permitir ser configurados, desactivados, desinstalados o inhabilitados por los usuarios que no tengan estas atribuciones para el ejercicio de sus funciones.
n) La Gerencia de Tecnologías de la información debe mantener los dispositivos móviles propiedad de COLPENSIONES con versiones estables y actualizadas de los sistemas operativos utilizados para su funcionamiento y de las aplicaciones en ellos instaladas.
o) La Gerencia de Tecnologías de la información debe implementar mecanismos para realizar monitoreo de los dispositivos móviles que se conectan a la red de COLPENSIONES.

4.13.4 Protección para dispositivo propio

Los siguientes son los lineamientos para el uso de dispositivos móviles que son propiedad de los colaboradores:

a) El uso de un dispositivo móvil personal por parte de un colaborador para acceder a los sistemas de información de COLPENSIONES está restringido, se podrá usar como apoyo a tareas bajo autorización del líder de proceso informando a la Gerencia de Tecnologías de la Información.
b) Los dispositivos personales deben conectarse a un segmento de red independiente -aislada de los segmentos de red de servidores y datos de la operación- dentro de la red de datos corporativa de COLPENSIONES.
c) Se debe asegurar que toda la actividad realizada en los sistemas de información de COLPENSIONES desde dispositivos personales, es registrada en logs en los cuales se puede tener su trazabilidad.
d) El uso del dispositivo móvil personal debe asegurar el cumplimiento de los lineamientos establecidos en las políticas de Seguridad de la Información definidas en el presente manual.
e) La Gerencia de Tecnologías de la información debe validar que el dispositivo cuente con software antimalware legal, instalado y actualizado.
f) El colaborador debe cumplir con la reglamentación vigente en materia de uso de software legal; es enteramente responsable de contar con todo el software de su dispositivo debidamente licenciado.

4.13.5 Política para la Seguridad de la Red

Aseguramiento de las redes cableadas e inalámbricas de COLPENSIONES, para garantizar la adecuada protección de la información de la entidad y el uso responsable de los recursos.

a) La Gerencia de Tecnologías de la Información debe determinar las necesidades de conectividad interna y externa en el cumplimiento de sus objetivos misionales y estratégicos, para garantizar la oportunidad, efectividad y eficiencia de las operaciones.
b) Las redes internas y las conexiones a redes externas deben ser gestionadas por la Gerencia de Tecnologías de la Información, para garantizar la seguridad de la informática y de los servicios de la entidad, y el uso responsable de los recursos.
c) La Gerencia de Tecnologías de la Información, debe mantener un mapa de red actualizado que contenga información detallada de los segmentos de red interna, zonas desmilitarizadas o DMZ, de las conexiones a Internet, con terceros a redes WAN y cualquier otro que se incluya dentro de la infraestructura de red de la entidad.
d) La Gerencia de Tecnologías de la Información debe definir las medidas de seguridad mínimas exigidas a los equipos que se conectarán a la red de la entidad. No se debe permitir la conexión de dispositivos que incumplan dichas medidas de seguridad.

- Definir y documentar las necesidades de conectividad de la entidad y proveer los recursos necesarios para suplirlas.
- Mantener actualizado el inventario de dispositivos de comunicaciones propiedad de COLPENSIONES, sus características y sus responsables asignados.
- Instalar, configurar y ubicar adecuadamente los dispositivos de comunicaciones y de red.
- Mantener copias de seguridad de la configuración de los dispositivos de comunicaciones de la entidad que por su criticidad así lo requieran.

e) La red de Colpensiones debe segmentarse y debe permitir identificar, controlar y monitorear el tráfico en toda la red.
f) Se debe garantizar la segmentación de entornos de desarrollo, pruebas, producción y los demás que se requieran, impidiendo el tráfico entre ellos y asegurando así los ambientes productivos. En los casos en que se requiera transportar información entre ambientes se deben usar aplicaciones o sistemas que permitan limitar el tráfico únicamente al estrictamente necesario.
g) Antes de aplicar cambios en dispositivos activos de la red de Colpensiones, estos deberán evaluarse, aprobarse y aplicarse en ambientes controlados.

h) Es responsabilidad de la Gerencia de Tecnologías de la Información mantener un ambiente pre productivo de la red para probar y aprobar los cambios antes de aplicarlos en los dispositivos productivos de red.
i) El tráfico entrante y saliente entre segmentos de red debe estar claramente identificado, justificado y controlado. No se permite tráfico de ningún tipo entre dos segmentos de red que no lo requieran.
j) El tráfico entrante y saliente entre las zonas desmilitarizadas hacia redes públicas o Internet o hacia segmentos de red internos debe estar claramente identificado, justificado y controlado por dispositivos tipo Firewall y preferiblemente con características avanzadas para la detección o prevención de intrusos (IDS o IPS).
k) Las políticas de firewall deben tener claramente identificadas y documentadas las direcciones de origen y destino, así como los puertos, protocolos o servicios permitidos. No podrán existir políticas de firewall con orígenes, destinos, puertos, protocolos o servicios no determinados o con comodines tipo ANY.
l) Está prohibida la utilización de dispositivos que hagan conexiones tipo puente o by pass entre zonas de red con distinto nivel de confianza. Todo el tráfico entre diferentes segmentos de red debe ser controlado por dispositivos tipo Firewall.
m) La Gerencia de Tecnologías de información a través del equipo de seguridad informática debe realizar inspecciones periódicas para la detección de AP no autorizados (rogue AP), dispositivos en modo promiscuo, honeypots vecinos, redes inalámbricas no autorizadas (dispositivos dentro del área irradiando otros SSID) así como AP con configuraciones de red incorrectas o inseguras.
n) Las inspecciones pueden realizarse mediante inspección física o mediante la utilización de analizadores de redes inalámbricas o sniffers.
o) Es responsabilidad de la Gerencia de Tecnologías de la Información definir y mantener guías de configuración segura (hardening) para los dispositivos de comunicaciones y de red de la entidad, monitorear los procedimientos y controles de seguridad sobre la red cableada e inalámbrica y Instalar y configurar adecuadamente los controles de restricción de tráfico.
p) La Gerencia de Tecnologías de la Información debe implementar medidas de seguridad para garantizar que el proceso de autenticación y el envío y recepción de tráfico se haga de manera cifrada evitando así comprometer las credenciales de autenticación y la información sensible.
q) No se permite conectar a la red de COLPENSIONES dispositivos móviles propios para conectarse a Internet, por medio de conexiones WIFI, bluetooth, cableadas o de cualquier otro tipo.
r) El tráfico desde y hacia redes públicas e internet debe preferiblemente ser enviado o recibido por dispositivos o equipos ubicados en zonas de red desmilitarizadas o DMZ.
s) Con el ánimo de garantizar el uso adecuado del recurso de Internet y la seguridad de la información y de los sistemas de información internos, se deben definir e implementar reglas de navegación en Internet, evitando el ingreso a páginas de correo electrónico, herramientas para intercambio de información diferentes a las dispuestas por la entidad y almacenamiento en la nube, pornografía, ocio, piratería, trata de personas, redes sociales, actividades al margen de la ley, hacking, virus y malware, encuestas, compras y otras que considere necesarias.

t) El uso de las redes de COLPENSIONES está limitado al cumplimiento de las responsabilidades que cada usuario tenga con la entidad y no para fines personales.

4.14 Política para la gestión de ciberseguridad

La ciberseguridad, entendida como “el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la Entidad” de acuerdo con la definición de la Circular 007 de 2018 de la Superintendencia Financiera de Colombia, se constituye en uno de los componentes de la Seguridad de la Información, en conjunto con la seguridad en los procesos, las personas y la infraestructura. A partir de esta base, se definen los siguientes lineamientos para la ciberseguridad en COLPENSIONES, teniendo en cuenta los activos de información que en la MAI en el campo "Modo en que se presenta la información" es Digital:

a) Los riesgos de Seguridad de la Información y ciberseguridad deben gestionarse siguiendo la Metodología de Gestión de Riesgos de Seguridad de la Información (Manual del Sistema Integral de Administración de Riesgos, Parte V Manual Sistema de Gestión de Riesgos de Seguridad de la Información y Ciberseguridad) establecida por COLPENSIONES.
b) Los roles y responsabilidades para la ciberseguridad se encuentran definidos en el documento Roles y Responsabilidades de Seguridad de la Información.
c) Todos los colaboradores de COLPENSIONES deben cumplir las políticas y procedimientos de Seguridad de la Información de la Entidad.
d) La Gerencia de Riesgos y Seguridad de la Información debe definir las políticas y procedimientos de Seguridad de la Información, así como la metodología de gestión de activos y gestión de riesgos de Seguridad de la Información, gestionar su aprobación, socializarlos a todos los colaboradores y partes interesadas, monitorear su cumplimiento y asegurar que se mantengan actualizados.
e) La Gerencia de Riesgos y Seguridad de la Información debe promover la conciencia y entendimiento de los riesgos de Seguridad de la Información y ciberseguridad dentro de la Entidad, la cual contemple un nivel mínimo de exigencia en el aprendizaje de herramientas de Seguridad de la Información y el desarrollo de destrezas contra ataques de ingeniería social, y en general, cualquier tipo de ataque de ciberseguridad.
f) La Gerencia de Riesgos y Seguridad de la Información, debe promover la cultura de Seguridad de la Información; en esa misma línea, debe asegurar que la Dirección de Talento Humano implemente los programas de capacitación con base en el alcance definido por la Gerencia de Riesgos.

g) La Gerencia de Riesgos y Seguridad de la Información, debe establecer los mecanismos para generar conciencia sobre los riesgos de Seguridad de la Información en afiliados, pensionados y usuarios de todos los servicios de la Entidad.
h) La Gerencia de Tecnologías de la Información, debe implementar los controles de seguridad que se identifiquen en los análisis de riesgos, en las etapas de análisis, diseño, desarrollo, pruebas e implementación de arquitectura de servicios, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información.
i) El acceso a los sistemas de información de COLPENSIONES debe hacerse desde dispositivos que cumplan con las políticas de Seguridad de la Información de la Entidad.
j) La Gerencia de Tecnologías de la Información es la encargada de definir las herramientas antimalware a ser utilizadas en COLPENSIONES a partir de un análisis detallado de las opciones que ofrece el mercado y las necesidades identificadas al interior de la Entidad.

4.15 Política para el desarrollo seguro

Los líderes de los procesos deben cumplir con la gestión para que se definan los requerimientos funcionales y no funcionales del software. Dentro de los requerimientos no funcionales se encuentran los de Seguridad de la Información que se deben establecer de acuerdo con los resultados del análisis de riesgos. La Gerencia de Tecnologías de la Información es la responsable de planificar, desarrollar y ejecutar las actividades relacionadas con desarrollos, actualizaciones e instalaciones de software y planificar la ejecución de pruebas funcionales y de seguridad de los sistemas nuevos o modificados antes de ejecutar la instalación en los entornos de producción. Los lineamientos de esta política son:

a) Los controles de Seguridad de la Información definidos en el análisis de riesgos, deben ser incluidos en los requerimientos para el desarrollo del software.
b) Se debe establecer la arquitectura de seguridad a partir de los requerimientos definidos.
c) Las funciones, componentes y controles de seguridad, deben ser descritos en detalle en el documento de arquitectura.
d) A partir de los requerimientos de seguridad, se deben definir y documentar, en la etapa de diseño, las pruebas a realizar para validar su cumplimiento, así como el resultado esperado.
e) Se debe asegurar que la información clasificada y reservada sea cifrada; el algoritmo a utilizar debe ser un algoritmo fuerte, es decir, uno para el cual no se hayan identificado vulnerabilidades a la fecha siguiendo el LINEAMIENTO CONTROLES CRIPTOGRÁFICOS GGT-PSE-LIN-008.
f) Se debe aplicar la Política de uso de controles criptográficos.

g) Todos los programas deben incluir la generación de registros de auditoría; cada registro debe incluir como mínimo, la identidad del usuario, la acción ejecutada, la fecha y hora del evento. Estos registros deben contar con controles que aseguren su integridad.
h) La Gerencia de Tecnologías de la Información debe ejecutar un análisis de vulnerabilidades del código fuente; se debe asegurar que las vulnerabilidades identificadas son remediadas.
i) Se debe definir y estandarizar el ciclo de vida y los criterios de desarrollo seguro, aplicando las buenas prácticas y lineamientos para restricciones de captura de datos, definición de variables y manejo de excepciones.
j) Toda modificación o actualización en el software, debe contar con un análisis de vulnerabilidades de código (estático y dinámico) previamente en ambientes independientes de desarrollo, calidad e integración, con el objetivo de identificar y remediar los defectos y vulnerabilidades, antes de pasar al ambiente de producción.
k) Se debe asegurar que todos los errores identificados en las pruebas de seguridad sean corregidos previo a la puesta en producción. Los resultados de las pruebas deben ser aprobados por el propietario del software y deben quedar debidamente documentados.
l) La documentación del software debe incluir las consideraciones de Seguridad de la Información para su uso.
m) La Gerencia de Tecnologías de la información, debe asegurar la independencia de los ambientes de desarrollo, pruebas, calidad y producción.
n) Se deben establecer controles de acceso independientes para cada uno de los ambientes previos (desarrollo, integración y calidad).
o) No se puede hacer uso de datos de producción en ambientes previos. En caso de requerir hacer uso de datos de producción para realizar pruebas, es necesario que se establezcan mecanismos para ofuscar, transformar y/o enmascarar los datos, los cuales deben ser aprobados por el propietario de la información.
p) No se debe permitir la ejecución de comandos del sistema operativo desde el software desarrollado o adquirido.
q) Se debe garantizar que el software en su funcionamiento e inclusive en situaciones de excepción, anormales o de falla, nunca entregue información clasificada o reservada (especificaciones de la tecnología utilizada, direcciones IP, rutas de acceso, nombres de archivos, nombres y versiones de aplicaciones de software, código fuente, información de errores y cadenas de conexión).
r) La Gerencia de Tecnologías de la Información debe establecer una gestión de vulnerabilidades técnicas orientada a analizar los problemas de seguridad (vulnerabilidades) que surgen en los productos de

software, que sean publicadas por los proveedores de tecnología y las agencias especializadas (CVE, OWASP) o detectados por cualquier usuario y proponer las medidas de mitigación al riesgo definido.

s) Establecer la identificación de vulnerabilidades técnicas para todas las librerías y demás componentes utilizados en el desarrollo de software.

t) No se deben dejar en comentarios o quemadas en el código del software las credenciales de acceso o autenticación.

u) No se deben dejar quemadas en el código direcciones IP o nombres de máquinas, estas deben poderse cambiar directamente en la configuración del software.

v) Crear la funcionalidad para que se asegure el cierre de las sesiones por desuso o tiempo de conexión; este tiempo debe ser establecido con base en los requerimientos funcionales definidos para la aplicación.

w) Se debe generar un acuerdo previo con desarrolladores y fábricas de software, el cual debe establecer la protección de la propiedad intelectual y la confidencialidad de la información gestionada en los proyectos de desarrollo.

x) Cualquier cambio que se ejecute durante el ciclo de vida de desarrollo, debe pasar por un control de cambios en donde se evalúen los riesgos de Seguridad de la Información.

y) No está permitido escribir o modificar código autocopiante o cualquier otro tipo de código malicioso, así como funciones u operaciones no documentadas o no autorizadas en los programas.

z) Se deberán tener las siguientes consideraciones con relación a los datos de entrada y salida de los sistemas de información:

- Realizar validaciones de datos de entrada y salida en un sistema confiable.
- Construir los aplicativos para que validen los datos de entrada y generen los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
- Validar las entradas de datos con una lista “blanca” que contenga un directorio de caracteres aceptados.
- Validar el intento de ingreso de bytes nulos, caracteres de nueva línea o caracteres de alteración de rutas.
- Limpiar las salidas de datos no confiables hacia consultas SQL, XML y LDAP o hacia comandos del sistema operativo.

aa) Se deben aplicar controles a las entradas como:

- Entrada dual y otros chequeos de entrada para detectar errores como valores fuera de rango, tipos de datos, longitud, caracteres inválidos en campos de datos, datos incompletos o faltantes, control de datos no autorizados o inconsistentes.
- Revisión periódica de contenidos de campos clave o archivos de datos para confirmar su validez e integridad.
- Procedimientos para responder a errores de validación.
- Procedimientos para determinar la veracidad de los datos de entrada.
- Crear registros (logs) de las actividades relacionadas con el proceso de entrada de datos.

Se deben aplicar controles de Procesamiento como:

El diseño e implementación de aplicaciones debe asegurar que los riesgos de fallas de procesamiento que llevan a pérdida de integridad son minimizados; esto incluye:

a) El uso de funciones de adición, modificación y borrado para realizar cambios en los datos.
b) Procedimientos para prevenir la ejecución de programas fuera de secuencia o cuando falla el procesamiento previo.
c) Uso de programas para recuperación de fallas, con el objeto de asegurar el procesamiento correcto de los datos.
d) Controles de lote (batch).
e) Controles de balanceo como corrida a corrida, totales de archivos actualizados.
f) Totales hash de registros y archivos.
g) Controles de integridad y autenticidad para datos que se cargan desde computadores remotos o en procesos en lotes.
h) Creación de registros (logs) de las actividades relacionadas con el procesamiento de datos.

Se deben establecer los siguientes controles para la autenticación en los sistemas de información:

- Toda aplicación debe cumplir con la Política de Control de Acceso.
- Validar los datos de autenticación, luego de haber completado todos los datos de entrada.

Se debe realizar enmascaramiento de contraseñas y códigos de acceso, al momento de su digitación por parte del usuario, para el ingreso a todo sistema de información o aplicación, asegurando que no puedan ser visualizados en pantalla.

Para el manejo de archivos se deberán acatar las siguientes consideraciones:

- Remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción (Sanitización).
- Prevenir la revelación de la estructura de directorios de los sistemas construidos.

Para el establecimiento de conexión a las bases de datos, se deberán considerar los siguientes aspectos:

- No incluir las cadenas de conexión a las bases de datos en el código de los aplicativos.
- Cerrar la conexión a las bases de datos desde los aplicativos, tan pronto como estas no sean requeridas

Para la puesta en producción:

- Se debe garantizar que la puesta en producción de un software, o su posterior mantenimiento, no comprometa los controles de seguridad existentes o introducir nuevas vulnerabilidades.
- Los desarrolladores no deben tener acceso a los entornos de producción.

a) La documentación de los desarrollos debe generarse durante el ciclo de vida de desarrollo, debe ser revisada por los usuarios finales, actualizarse si cambia alguna de las funcionalidades y almacenarse en un servidor administrado por la Gerencia de Tecnologías de la Información.
b) La Gerencia de Tecnologías de Información debe asegurar la conservación de las versiones de software con su respectiva documentación, así como la disponibilidad de los instructivos necesarios para su restauración en caso de requerirse.
c) Los comentarios escritos por los desarrolladores en el programa fuente, no deben divulgar innecesariamente la información de configuración.
d) El software desarrollado para COLPENSIONES, debe realizarse por medio de herramientas y/o software licenciado.
e) Se debe cumplir con los términos y condiciones para el software obtenido, tanto comercial como código abierto.
f) Se debe verificar el cumplimiento de los derechos de autor y los derechos de patentes, de acuerdo con los términos de aceptación de la licencia.

g) Se debe mantener un registro actualizado del software utilizado por COLPENSIONES y el número de licencias autorizadas y controlar su cumplimiento.

4.16 Política para gestión de medios de almacenamiento

Los siguientes son los lineamientos definidos por COLPENSIONES para la gestión de medios de almacenamiento:

a) La Dirección de Gestión Documental debe implementar los controles de seguridad que los propietarios de la información determinen, sobre los activos que esta Gerencia custodia.

4.16.1 Gestión de medios removibles

Para medios removibles, se deben aplicar las siguientes directrices:

a) Se debe asegurar el cumplimiento para manejo de medios definido por parte de la Dirección Documental Ver. Instructiva administración de medios magnéticos. Código GAO-GDO-INS-015.
b) El propietario de la información define qué activos se permiten almacenar en medios removibles y bajo qué condiciones; de cualquier manera, la información reservada y clasificada debe permanecer cifrada.
c) Los medios removibles con información de COLPENSIONES sólo pueden ser utilizados en dispositivos que cumplan las políticas de Seguridad de la Información de la Entidad.
d) Se debe eliminar la información del medio removible provisto por COLPENSIONES tan pronto sea utilizada para el fin para el cual fue copiada en él y de acuerdo con los tiempos de retención establecidos en la TRD, de forma que no pueda ser recuperable. Ver Instructivo administración de medios magnéticos. Código GAO-GDO-INS-015
e) Se debe solicitar autorización por parte de los propietarios de los activos para retirar los medios de la Entidad, dejar registro de estos retiros con el fin de mantener un rastro de auditoría.
f) La información contenida en medios removibles debe cumplir con lo establecido por la Dirección de Gestión Documental. Ver. Instructiva administración de medios magnéticos. ADMINISTRACIÓN DE MEDIOS MAGNÉTICOS. Código GAO-GDO-INS-015
g) La información en el momento en que ya no resulte de utilidad para COLPENSIONES y cuando se haya cumplido el período de retención exigido por ley, reglamento o contrato, debe ser destruida conforme a las tablas de retención documental. Para toda destrucción de información se debe dejar acta firmada

por el propietario de la información y dejar constancia en la Gerencia de Riesgos y Seguridad de la Información y Ciberseguridad.

h) Para el envío de medios físicos a través del servicio postal o empresas de mensajería se debe cumplir con lo establecido por la Dirección de Gestión Documental.

i) La Gerencia de Tecnologías de la Información es el área encargada de la disposición final de medios de almacenamiento provistos por la Entidad, asegurando que la información contenida en ellos no sea recuperable.

4.17 Política para la concienciación en Seguridad de la Información y ciberseguridad

COLPENSIONES entiende que las personas son a menudo la mayor vulnerabilidad para la Seguridad de la Información ya que son consideradas el eslabón más débil en la cadena de controles que salvaguardan la integridad, confidencialidad y disponibilidad de la información de la Entidad. Por lo anterior, hará todo lo posible para garantizar que todos los colaboradores conozcan y cumplan las políticas del SGSI.

a) Todos los colaboradores de COLPENSIONES deben ser capacitados y evaluados en la aplicación de las políticas y procedimientos de Seguridad de la Información.

b) La capacitación en Seguridad de la Información debe iniciar en el momento de la vinculación del colaborador a COLPENSIONES.

c) Todos los colaboradores de COLPENSIONES deben conocer los mecanismos para identificar, informar y prevenir posibles incidentes de seguridad. Ver Instructivo Gestión de incidentes de Seguridad de la Información y ciberseguridad, AGE-GRI-INS-002

d) **La Gerencia de Riesgos y Seguridad de la Información** deben ejecutar campañas de seguridad periódicas, al menos una vez por año, en las que se busque la continua toma de conciencia de los colaboradores de la Entidad con la Seguridad de la Información.

e) Dentro de las campañas de toma de conciencia y capacitaciones, se debe informar a los colaboradores el marco legal y regulatorio referente a Seguridad de la Información.

f) La asistencia a las sesiones de capacitación y sensibilización en Seguridad de la Información es de carácter obligatorio.

g) La evaluación del conocimiento en Seguridad de la Información requerido para los colaboradores está a cargo de la Dirección de Talento Humano.

h) Se debe conservar las evidencias de la participación de los colaboradores en las capacitaciones y evaluaciones de Seguridad de la Información.

i) El resultado de las evaluaciones debe ser analizado por parte de la Gerencia de Riesgos de Seguridad de la Información para realizar un diagnóstico y determinar las acciones pertinentes encaminadas a generar la cultura de Seguridad de la Información que la Entidad requiere.

4.18 Política para gestión de vulnerabilidades

Una gestión eficiente de vulnerabilidades, permite a COLPENSIONES actuar de manera oportuna para prevenir riesgos de Seguridad de la Información, por eso establece los siguientes lineamientos:

a) El Grupo de Seguridad Informática de la Gerencia de Tecnologías de la Información, debe ejecutar periódicamente el proceso definido para la gestión de vulnerabilidades. ver. Subproceso Gestión de Vulnerabilidades código GGT-PSE-CAP-001.
b) El responsable del Software (*Roles y Responsabilidades de Seguridad de la Información)* debe cumplir con el Procedimiento de Gestión de Vulnerabilidades GGT-PSE-CPR-002.
c) Se debe determinar la necesidad de ejecutar pruebas de hacking ético como resultado de los análisis de riesgos de Seguridad de la Información; se debe definir también la periodicidad con la cual se deben hacer. Se debe asegurar la total independencia entre el desarrollador del software y quién realiza las pruebas.
d) El Grupo de Seguridad Informática de la Gerencia de Tecnologías de la Información, debe revisar Trimestralmente y hacer seguimiento, al reporte de nuevas vulnerabilidades técnicas que puedan afectar los sistemas de información y aplicaciones de COLPENSIONES; en caso de identificar una vulnerabilidad, debe informar a los propietarios de la información, a los responsables del software y a los administradores de la plataforma tecnológica, y definir el plan de acción para su gestión. Lo anterior teniendo en cuenta el procedimiento Gestión de Vulnerabilidades asignado al proceso GESTIÓN DE PROVISIÓN DEL SERVICIO DE TI
e) En los casos que el responsable del Software o la aplicación esté a cargo de un proveedor se debe asegurar a través del contrato, que se informe acerca de la identificación de una nueva vulnerabilidad tan pronto como esta se identifique, indicando los posibles efectos que puede tener, el plazo para contar con el parche que la soluciona y las medidas que debe tomar la Entidad mientras este se desarrolla.
f) Una vez notificado de la existencia de una vulnerabilidad, el propietario de la información debe cumplir con la debida diligencia para la protección de la confidencialidad, integridad y disponibilidad de sus activos, de acuerdo con la matriz de riesgos de Seguridad de la Información de su proceso.
g) COLPENSIONES debe contar con un proceso para la gestión de vulnerabilidades técnicas que asegure la identificación oportuna de una vulnerabilidad y el plan de respuesta respectivo. Ver procedimiento

Gestión de Vulnerabilidades asignado al proceso Gestión Provisión de Provisión del Servicio TI código GGT-PSE-CAP-001

h) El grupo de Seguridad Informática **debe** realizar escaneos de vulnerabilidades de forma periódica, al menos mensual, sobre el software de la Entidad; los resultados deben reflejar qué activos de información pueden verse afectados para cada una de las vulnerabilidades detectadas.

i) Generar de manera automática por lo menos 2 veces al año un informe consolidado de las vulnerabilidades encontradas. Los informes de los últimos 2 años deben estar a disposición de la SFC.

j) Para la generación de los informes solicitados se debe tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre.

k) Las herramientas usadas en el análisis de vulnerabilidades, deben estar homologadas por el CVE (Common Vulnerabilities and Exposures) y actualizadas a la fecha de su utilización.

l) Para los escaneos, se debe realizar un análisis diferencial de vulnerabilidades, comparando el informe actual con respecto al inmediatamente anterior.

m) El Plan de remediación de vulnerabilidades debe construirse entre el Grupo de seguridad informática, el propietario de la información y el responsable del software, priorizando las vulnerabilidades que puedan afectar los activos de información y/o servicios más críticos.

n) La criticidad de una vulnerabilidad se valora bajo los siguientes criterios:

- **Crítica:** Un atacante interno o externo podría fácilmente tomar control de un activo de información / Activo de TI que puede conducir al compromiso de la red. Normalmente son vulnerabilidades explotables remotamente, que pueden generar un compromiso del sistema. La explotación exitosa normalmente no requiere ninguna interacción y la explotabilidad es común.

- **Alta:** Un atacante interno o externo podría obtener el control de un activo de información / activo de TI. Puede haber una pérdida potencial de información altamente sensible. Típicamente utilizado para vulnerabilidades remotamente explotables que pueden conducir a un compromiso del sistema. La explotación normalmente no requiere ninguna interacción, pero no hay exploits conocidos disponibles.

o) Los dispositivos que se conecten a la red de COLPENSIONES deben pasar por un proceso de hardening y análisis de vulnerabilidades realizado por la Gerencia de Tecnologías de la Información aplicando el LINEAMIENTO DE SEGURIDAD PARA EL ACCESO A REDES INALAMBRICAS CORPORATIVAS GGT-PSE-LIN-004 y GUIA PARA CONFIGURACIÓN DE CONEXIÓN A LA RED INALAMBRICA TERCEROS A COLPENSIONES GGT-GSO-GUI-038.

4.19 Política de gestión de cambios tecnológicos en COLPENSIONES

Se debe contar con un análisis de riesgos de Seguridad de la Información como requisito para la presentación de un cambio, o una liberación de una solución tecnológica, el cual debe ser realizado siguiendo la Metodología de Gestión de Riesgos de Seguridad de la Información (Parte V Manual Sistema de Gestión de Riesgos de Seguridad de la Información y Ciberseguridad AGE-GIR-MAN-013). El procedimiento Gestión de Liberaciones debe asegurar que los riesgos identificados se encuentran dentro del apetito de riesgo de la Entidad, caso contrario, se debe contar con el soporte de la aceptación del riesgo por parte del propietario de la información.

4.20 Política para el licenciamiento y uso de software

Se definen los siguientes lineamientos para el licenciamiento y uso de software:

a) La Gerencia de Tecnologías de la Información es la única área autorizada para instalar, desinstalar, configurar, probar, activar o inactivar en producción cualquier tipo de software.
b) Sólo los administradores de sistemas de información autorizados por la Gerencia de Tecnologías de la Información podrán realizar la instalación de software en los equipos de la Entidad, siguiendo el INSTRUCTIVO PARA LA GESTIÓN DE EQUIPOS GGT-GSO-INS-015.
c) La Gerencia de Tecnologías de la Información es la responsable por definir, actualizar e informar la lista de software autorizado en la Entidad.
d) La Gerencia de Tecnologías de la Información debe implementar controles para asegurar que el software utilizado en COLPENSIONES es el autorizado.
e) La Gerencia de Tecnologías de la Información únicamente puede implementar los requerimientos de seguridad que el responsable del software haya autorizado.
f) La Gerencia de Tecnologías de la Información es la única dependencia autorizada para la adquisición de software y hardware; las demás dependencias deben gestionar su adquisición a través de esta área. Ver. Manual de contratación 2021 página web COLPENSIONES https://www.colpensiones.gov.co/documentos/536/04-manual-de-contratacion/
g) La Gerencia de Tecnologías de la Información debe presentar a la Oficina de Control Interno el reporte sobre el cumplimiento de las normas de propiedad intelectual y derechos de autor, para dar cumplimiento a los requerimientos de los organismos de control relacionados con el uso adecuado de software en COLPENSIONES.
h) La Gerencia de Tecnologías de la Información debe asegurar que los productos de software adquiridos sean formalmente entregados a COLPENSIONES; se debe contar con el soporte de esta entrega la cual

debe incluir los medios de instalación, así como la documentación de la licencia, propiedad y derechos de uso.

i) El retiro de un software es decisión del responsable del Software; en el momento que se tome esta decisión, debe realizar el requerimiento a la Gerencia de Tecnologías de la Información.

4.21 Política de seguridad para equipos de cómputo

Se definen los siguientes lineamientos para la Seguridad de la Información en los equipos de cómputo:

a) Los equipos de procesamiento y almacenamiento de información diferentes a los computadores asignados a los colaboradores, así como los equipos de comunicaciones, deben estar ubicados en áreas específicamente diseñadas para tal fin, las cuales deben cumplir los lineamientos para áreas seguras establecidos en la Política de Control de Acceso.
b) Los computadores asignados a los colaboradores son para uso exclusivo de las funciones del cargo que desempeñan en la Entidad.
c) Los computadores portátiles asignados a los colaboradores de COLPENSIONES deben ser entregados con guaya de seguridad.
d) Es responsabilidad de cada colaborador al que se asigne un equipo portátil, mantenerlo anclado haciendo uso de la guaya de seguridad suministrada por la Gerencia de Tecnologías de la Información.
e) La Gerencia de Tecnologías de la Información debe realizar mantenimientos preventivos a computadores portátiles, de escritorio y servidores con la periodicidad y especificaciones recomendadas por los fabricantes; se debe mantener el registro de los mantenimientos realizados y de las fallas detectadas.
f) Todos los equipos de cómputo de la Entidad deben tener instalados los parches de seguridad más recientes proporcionados por los fabricantes. La aplicación de los parches debe realizarse por la Gerencia de Tecnologías de la Información tan pronto como sean liberados por el fabricante.
g) La salida de equipos de las instalaciones de COLPENSIONES debe ser autorizada por el responsable del área a la cual esté asignado el equipo.
h) Toda información de COLPENSIONES debe ser removida de un equipo antes de su disposición, reasignación, cambio de uso, venta o donación, usando técnicas para hacer que la información original no sea recuperable de acuerdo con la GUIA BORRADO SEGURO HERRAMIENTA DBAN GGT-GSO-GUI-042 y el documento LINEAMIENTOS Y ESTANDARES DEL GOBIERNO Y GESTIÓN DE TI GGT-GRN-LIN-001.

i) Cualquier configuración sobre los computadores asignados a los colaboradores de COLPENSIONES, sólo puede ser realizada por la Gerencia de Tecnologías de la Información; ningún colaborador diferente está autorizado para realizar este tipo de tareas.
j) El acceso a unidades de CD, DVD y dispositivos USB en los computadores asignados a los colaboradores de COLPENSIONES, por defecto, debe ser restringido; en caso de ser necesaria su habilitación por necesidades propias del rol del colaborador, esta debe ser solicitada por el responsable del área y ejecutada por la Gerencia de Tecnologías de la Información.
k) No está permitido a los colaboradores mover o reubicar los equipos de cómputo pertenecientes a la Entidad, retirar marcas, logotipos ni hologramas de los mismos sin la autorización de la Gerencia Administrativa.
l) No está permitido a los colaboradores abrir o destapar los equipos de cómputo de COLPENSIONES. Sólo el personal de la Gerencia de Tecnologías de la Información está autorizado para realizar esta labor.
m) Los colaboradores deben cerrar la sesión de sus computadores cuando no se encuentren en su lugar de trabajo.
n) La Gerencia de Tecnologías de Información es la única autorizada para la instalación de equipos de comunicaciones en las instalaciones de COLPENSIONES, a través de los procesos y procedimientos oficialmente definidos; estos dispositivos incluyen entre otros: access points, piñas, repetidores, equipos para análisis de tráfico.
o) La implementación de controles físicos para proteger los equipos de cómputo de los colaboradores en las instalaciones de COLPENSIONES es responsabilidad de la Gerencia Administrativa.
p) Se debe establecer una línea base para los computadores asignados a los colaboradores y se debe asegurar su aplicación, de manera que sólo esté instalado el software autorizado y que cuenten con las herramientas de protección de seguridad definidas por la Gerencia de Tecnologías de Información.
q) Todos los equipos asignados a los colaboradores deben ser devueltos a COLPENSIONES una vez finalizada la relación contractual.

4.22 Política de escritorio limpio y pantalla limpia

Se debe proteger la información impresa, almacenada en medios removibles y visible en la pantalla de los equipos informáticos para que su acceso solo sea permitido a las personas autorizadas de acuerdo con la Política de Control de Acceso. Los lineamientos definidos son:

a) Todos los equipos de cómputo deben tener configurado el cierre automático de sesión por inactividad; el tiempo será determinado por el Grupo de Seguridad Informática de la Gerencia e Tecnologías de la Información.
b) Los colaboradores no deben dejar visibles en el escritorio físico documentos clasificados o reservados.
c) Los colaboradores deben borrar la información reservada y clasificada escrita en los tableros de las salas de reuniones.
d) Los colaboradores deben mantener los documentos y medios de almacenamiento removibles en los lugares destinados para este propósito como son escritorios, archivadores y demás que apliquen. Estos elementos solo pueden estar por fuera de estos sitios cuando estén siendo usados por la persona autorizada, una vez termine la actividad se debe guardar inmediatamente.
e) La impresión de documentos con información clasificada o reservada sólo se debe permitir cuando esté contemplada en el uso aceptable del activo de información. Una vez se imprima, debe asegurarse que se retira el documento en forma inmediata de la impresora o equipo destinado para esta tarea.
f) Se debe asegurar que cuente con el marcado de la clasificación registrada en la matriz de activos de información.
g) Se debe bloquear la pantalla del equipo de cómputo cada vez que el usuario no se encuentre trabajando sobre éste.
h) No manipular líquidos o comida sobre el escritorio en el que se encuentra el computador del colaborador.
i) La pantalla del computador (escritorio) no debe contener ningún tipo de archivo; sólo son permitidos los accesos directos a las aplicaciones necesarias para que los colaboradores ejerzan sus funciones y obligaciones contractuales.
j) El personal de seguridad física debe monitorear el cumplimiento de las políticas relacionadas con la protección física de equipos de cómputo.

4.23 Política para la transferencia de información

Para el cumplimiento de sus obligaciones COLPENSIONES intercambia información con diferentes entes y por diferentes medios. La transferencia de información por cualquier medio debe realizarse protegiendo la confidencialidad e integridad de los datos con los mecanismos acordes con la clasificación del activo de información involucrado. Para COLPENSIONES se debe dar cumplimiento a los siguientes lineamientos:

4.23.1 Directrices de intercambio de información entre personal de COLPENSIONES

a) Quien tenga la necesidad de enviar información con datos personales, debe confirmar que cuenta con la autorización expresa del titular del dato o su representante para su tratamiento. Ver Manual de lineamientos y procedimientos de protección de datos personales. https://www.colpensiones.gov.co/documentos/714/manuales/
b) Sólo se puede realizar intercambio de información de COLPENSIONES cuando dicho intercambio corresponda a actividades relacionadas con el desarrollo de sus funciones.
c) Para el intercambio de información se debe aplicar lo establecido por el propietario de la información de acuerdo con la política de uso aceptable correspondiente.
d) Siempre que se realice intercambio de información catalogada como Pública Clasificada o Pública Reservada, dicho intercambio debe ser aprobado por el jefe directo o supervisor de contrato.
e) Se debe seguir el Procedimiento para transferencia de información de COLPENSIONES.

4.23.2 Directrices de intercambio de información con terceros.

a) Se debe cumplir con lo establecido en la política de uso aceptable definida por el propietario de la información.
b) Se debe restringir el intercambio de información impresa con terceros considerando las vulnerabilidades que este medio trae.
c) Todo el intercambio debe guardar una trazabilidad para auditorías, reportes a entes de control o una potencial gestión de incidentes de Seguridad de la Información.
d) El intercambio de información reservada o clasificada debe estar protegido con cifrado.
e) El intercambio de información clasificada con nivel alto de integridad debe estar protegido con firma digital.

4.24 Política de uso de controles criptográficos

Se debe hacer uso de algoritmos criptográficos fuertes, es decir aquellos para los que en la fecha de aplicación no tengan vulnerabilidades, para proteger la confidencialidad e integridad de la información; todas las partes interesadas en el alcance deben cumplir con los lineamientos de controles criptográficos GGT-PSE-LIN-008 y las siguientes directrices:

a) El uso de controles criptográficos únicamente es válido cuando sea el resultado de un análisis de riesgos y su implementación sea autorizada por el propietario de la información correspondiente.

b) Se debe cifrar en almacenamiento y en tránsito la información catalogada como clasificada o reservada, de acuerdo con el resultado del análisis de riesgos.
c) Las contraseñas de acceso a los sistemas de información, sólo pueden almacenarse o transmitirse haciendo uso de controles criptográficos.
d) Se debe firmar digitalmente la información con nivel de clasificación Alto para Integridad según GUÍA GESTIÓN DE CERTIFICADOS DE FIRMA DIGITAL - GGT-PSE-GUI-008
e) Para realizar la distribución de la contraseña de cifrado de un archivo, esta debe hacerse a través de un medio diferente al del envío de este.
f) Por defecto, se hará uso de algoritmos de cifrado asimétrico y se permitirá el uso de algoritmos de cifrado simétrico solo para VPNs.

4.25 Política de trabajo en casa – Conexión Remota Externa

Con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información en un entorno de trabajo en casa, los colaboradores autorizados, deben mantener los controles de Seguridad de la Información establecidos para los activos de información requeridos en este entorno, verificando el cumplimiento de las políticas de Seguridad de la Información.

4.25.1 Directrices de seguridad para todo el personal

a) Para cualquiera de los colaboradores de la Entidad, debe estar autorizado por el jefe o supervisor inmediato, la Gerencia de Talento Humano y Relaciones Laborales, así como la Gerencia de Tecnologías de la Información, especificando los siguientes datos:

- Nombre del colaborador.
- Cargo del colaborador.
- Razón por la que se requiere el trabajo en casa.
- Fecha desde cuándo se requiere el trabajo en casa.
- Fecha hasta cuándo se hará uso del trabajo en casa.
- Definir los días de la semana y el horario en el que se hará uso del trabajo en casa.
- Especificar las aplicaciones que van a ser usadas.

b) El jefe inmediato debe validar que los requerimientos solicitados están acordes a las funciones asignadas al cargo que se formaliza en la Gerencia de Talento Humano.
c) El equipo utilizado puede ser:

- Computador asignado por COLPENSIONES, provisto con el licenciamiento para todo el software utilizado.
- Escritorio Virtual: software que permite el acceso a los datos de un servidor desde un equipo que únicamente brinda la interfaz requerida.
- Cliente de VPN: software que cuenta con la opción de acceso a los servicios.

4.25.2 Directrices de configuraciones de seguridad

En general se deben aplicar todas las políticas de Seguridad de la Información y Ciberseguridad de COLPENSIONES que sean pertinentes; se hace énfasis en los siguientes aspectos:

a) No es permitido que la sesión establecida con COLPENSIONES sea utilizada por una persona diferente al colaborador autorizado.
b) No iniciar sesión desde un sitio de acceso público.
c) Se deben considerar los requerimientos de seguridad definidos en el presente documento para los activos de información involucrados, es decir aplicar todas las restricciones y protecciones para la confidencialidad, integridad y disponibilidad definidas.

4.26 Política de gestión de llaves criptográficas

Proteger la confidencialidad, integridad y disponibilidad de las llaves criptográficas aplicando las siguientes directrices:

a) Las llaves criptográficas deben ser almacenadas en forma cifrada sin excepción alguna.
b) Cada vez que sea activada una llave criptográfica, será asignada a un colaborador de acuerdo con sus funciones y éste se convierte en Custodio de este activo de información y por ningún motivo puede compartir o delegar su uso.
c) La solicitud de llaves criptográficas debe realizarse formalmente a través de la Mesa de servicio.
d) Se debe mantener el registro de todas las operaciones con las llaves criptográficas, como son: creación, asignación, activación, desactivación y eliminación.
e) Si las llaves se almacenan en medios extraíbles, el responsable asignado debe garantizar su custodia permanente cuando no se encuentren en el medio destinado para su almacenamiento.
f) Las llaves solo pueden almacenarse en servidores o computadores de usuario autorizados para este propósito.

g) Cuando se considere que una llave puede estar comprometida por acceso no autorizado, se debe iniciar la gestión del incidente de seguridad de acuerdo con lo establecido por la Entidad. La revocación de las llaves es responsabilidad de la Gerencia de Tecnologías de la Información y esto se lleva a cabo cuando se concluya que es la acción para seguir como parte del tratamiento de un incidente de Seguridad de la Información acorde con las Políticas de Seguridad de la Información.
h) El cambio o actualización de las llaves debe ser solicitado por el jefe del custodio.
i) Se debe contar con un acta de entrega en la cual se registren los datos correspondientes al nombre del colaborador quien recibe la llave, fecha de entrega y su vigencia.

4.27 Política de seguridad en la nube

COLPENSIONES está comprometida con la protección integral de su información, bien sea que se encuentre en sus instalaciones o en las de un tercero, por tal motivo busca garantizar que todo tipo de información que sea almacenada, procesada, creada y/o eliminada en la nube, cuente con los controles de protección para la integridad, confidencialidad y disponibilidad de esta.

a) El contrato o licencia de alquiler en la nube, sin importar el tipo de plataforma, infraestructura o servicio, debe ser revisado y tener el visto bueno de la Oficina Asesora de Asuntos Legales.
b) Si la información va a ser accedida por dispositivos externos a la Entidad, es necesario verificar su compatibilidad con la Política de dispositivos para movilidad y acceso remoto.
c) Toda plataforma, servicio o infraestructura de nube con la que cuente la Entidad, debe contar con logs de auditoría.
d) Se debe restringir y monitorear el acceso a la nube privada mediante dispositivos de acceso restringido a nivel de infraestructura como Firewalls, IDS, IPS, etc.
e) Se debe configurar el servicio de nube para que la información sólo sea accedida y consultada desde un lugar geográfico específico.
f) El proveedor de servicios en la nube debe contar con controles que garanticen la confidencialidad, integridad y disponibilidad de la información.
g) Se debe asegurar que todo servicio de computación en la nube se diseñe, implemente y opere conforme a las políticas de Seguridad de la Información y ciberseguridad de COLPENSIONES.
h) El personal de COLPENSIONES debe cumplir las políticas de uso aceptable (AUP) del proveedor de servicio en la nube.
i) Se debe hacer un análisis de riesgos de Seguridad de la Información como prerrequisito para el despliegue de un servicio en la nube, el cual debe seguir la Metodología de Análisis de Riesgos de Seguridad de la Información de COLPENSIONES.

j) Las auditorías de Seguridad de la Información deben cubrir los servicios en la nube, lo cual debe quedar estipulado en el contrato con el proveedor del servicio.
k) La autenticación y autorización de usuarios en los servicios en la nube debe estar delegada en los sistemas de información de COLPENSIONES destinados para tal fin, de esta manera, es COLPENSIONES la encargada de gobernar el acceso, nunca el proveedor.
l) Los accesos de usuarios de COLPENSIONES a las consolas de administración de los servicios en la nube y sus interfaces, deben contar con autenticación de múltiple factor (MFA).
m) Se debe asegurar que los proveedores cumplan con los lineamientos de controles criptográficos GGT-PSE-LIN-008s.
n) Los controles definidos para los activos de información, deben aplicarse indistintamente para que estos se procesen y/o almacenen de forma local o en la nube.
o) En caso de contratar un servicio en la nube con almacenamiento de datos personales en un país diferente a Colombia, se debe garantizar que este país cumpla con los requerimientos exigidos por la ley 1581 de 2012.
p) El acceso a información de COLPENSIONES en la nube, debe hacerse desde equipos que cumplan las políticas de Seguridad de la Información de la Entidad.
q) El acceso a información de COLPENSIONES en la nube se debe hacer con base en el uso aceptable de cada activo definido por su propietario.
r) COLPENSIONES debe reconocer cuál es la ubicación de sus datos en la nube, en cada etapa del ciclo de vida, asegurando el cumplimiento de la legislación y regulación colombiana.
s) El propietario de la información debe contar con las herramientas para monitorear sus activos de manera que pueda conocer en cualquier momento quien accede a ella, cómo lo hace y qué acción realiza.
t) El propietario de la información debe contar con las herramientas para monitorear los controles implementados sobre sus activos de información.

4.28 Política de copias de respaldo

COLPENSIONES considera que la información de sus sistemas de información en producción, debe ser respaldada periódicamente, de manera que pueda recuperarse en caso de una contingencia.

Dentro de la información para la cual se deben mantener copias de seguridad se encuentran: bases de datos, software de aplicaciones, sistemas operativos, software base de la Entidad, buzones de correo, códigos fuente.

Se definen los siguientes lineamientos de copias de seguridad:

a) La Gerencia de tecnologías de la información es el área encargada de definir las especificaciones técnicas para asegurar la prestación del servicio de copias de respaldo, para lo cual debe evaluar las alternativas disponibles en el mercado que cumplan contractualmente con las especificaciones técnicas requeridas por Colpensiones.

b) Se tienen los siguientes tipos de backup, sin embargo, estarán definidos por la Gerencia de Tecnologías de la Información para COLPENSIONES:

- Completo: se copian todos los datos e información cada vez que se realiza el back up.
- Incremental: en el primer back up se copian todos los datos e información; en los posteriores, sólo se almacenan los cambios realizados desde el último back up.
- Diferencial: en el primer back up se copian todos los datos e información; en los posteriores, se almacenan los cambios realizados con relación al primer back up.

c) El propietario de la información debe determinar el tipo de backup a realizar: Full, incremental o diferencial y la periodicidad: diaria, semanal o mensual de acuerdo con la definición de la Gerencia de Tecnologías de la Información para atender los requerimientos de los procesos.
d) La presente política aplica para el respaldo de información en todos los repositorios oficiales de COLPENSIONES, lo cual incluye Data Center, nube u otros.
e) En las situaciones donde el activo de información a respaldar está categorizado como público clasificado o público reservado, las copias de respaldo deben ser cifradas.
f) Las copias de respaldo deben mantener los controles criptográficos de la información original.
g) Sólo se realizan copias de respaldo de los activos de información que previamente hayan sido identificados y valorados acorde con la Metodología para la identificación, clasificación y valoración de activos de información.
h) Las copias de respaldo de los equipos asignados a los colaboradores de COLPENSIONES se deben almacenar en el servidor de archivos creado para tal fin, en la carpeta definida en las tablas de retención documental.
i) Toda copia de respaldo debe llevar asociada una descripción, definido por la Gerencia de Tecnologías de la Información, la cual puede contener como mínimo:

- Label de cinta o Código de referencia: Información de identificación única para cada copia de respaldo.
- Tipo de backup: Full, incremental o diferencial.
- Contenido: Descripción general del contenido de la copia de seguridad.
- Fecha y hora: De la realización del backup.
- Custodio: Responsable por resguardar las copias de back up aplicando los controles definidos.
- Se debe llevar un registro en una bitácora, adicionando el proveedor a quien se entrega para su custodia.

j) El propietario de la información debe definir la frecuencia de realización de las copias de respaldo, la cual debe estar determinada por el análisis de riesgos, ésta toma como insumo las necesidades de negocio, así como los requerimientos normativos, legales y reglamentarios. Esta información debe estar alineada con las Tablas de Retención Documental y el Análisis de Impacto del Negocio (BIA).

k) La Gerencia de Tecnologías de la Información a través de la Dirección de Infraestructura, debe realizar de forma periódica, la validación aleatoria de las copias de respaldo de los sistemas de información críticos de la Entidad.

l) Se deben mantener registros de la realización de los procesos de revisión y restauración de la información, como parte del proceso.

m) La Gerencia de Tecnologías de la Información a través de la Dirección de Infraestructura, es el área responsable por ejecutar las copias de respaldo de acuerdo con los requerimientos del propietario de la información; es responsable también por la implementación de los controles para su custodia, así como de mantener un registro o inventario actualizado de las copias de respaldo ejecutadas, y cuáles han sido utilizadas para restauración.

n) El almacenamiento de las copias de respaldo debe realizarse bajo condiciones físicas que aseguren la protección contra accesos no autorizados. Sólo personal autorizado por la Gerencia de Tecnologías de la Información, podrá acceder y manipular los medios de soporte y respaldo de información.

o) Las condiciones ambientales del lugar de almacenamiento de las copias de respaldo deben cumplir las especificaciones del fabricante, estándares y buenas prácticas del mercado.

p) Los lugares de almacenamiento de las copias de respaldo deben presentar, bajo nivel de riesgo de incendio, inundación, contaminación química o electromagnética.

q) Si las copias de almacenamiento son resguardadas por un tercero, se debe contar con el registro de la fecha de entrega y de su ubicación; si se va a hacer un cambio de ubicación, sólo puede realizarse previa autorización de COLPENSIONES, y se deben registrar los detalles de la novedad.

r) Los medios de almacenamiento de información deben ser eliminados de forma segura al final de su vida útil o al alcanzar el número máximo de usos recomendado por el fabricante. Para tal efecto debe realizar la destrucción de los medios de forma física, o el borrado seguro. En el evento que se active el proceso de destrucción y/o eliminación de los medios de almacenamiento, se debe dejar registro de dicha actividad, mediante un acta.

5. Excepciones

Si se presenta una situación que requiera una excepción que lleve al incumplimiento de una política de Seguridad de la Información, se deben documentar las condiciones sobre las cuales se presenta y especificar las circunstancias que justifican la decisión. Cada excepción conlleva un riesgo que debe tener un responsable, quien asume esta posición frente al Comité Integral de Riesgos, con la asesoría del Grupo de Seguridad de la Información que presentará el panorama de la situación.

6. Incumplimiento de Políticas y Lineamientos de Seguridad de la Información y Ciberseguridad

El incumplimiento de cualquiera de las políticas y lineamientos del presente documento, deben ser reportados a la Oficina de Control Disciplinario Interno para investigación de las conductas de los colaboradores de la entidad que puedan transgredir la normatividad interna y/o externa, y fallar los procesos disciplinarios de conformidad con lo dispuesto en el régimen disciplinario.

7. Control de cambios del documento

FECHA	VERSIÓN	MODIFICACIÓN	ELABORÓ	REVISÓ.	APROBÓ.
15/06/2019	1.0	Creación inicial	Nombre: Liliana Serrano Cargo: Asesor Vicepresidencia	Nombre: Antonio José Coral Triana Cargo: Gerente de riesgos y Seguridad de la información	Nombre: Fabián Mauricio Arias Cargo: Vicepresidente de Seguridad y Riesgos Empresariales
15/03/2020	2.0	Modificación de XI cláusulas Y Adición XIV capítulos	Nombre: Marysol Kattah Cargo: Profesional Máster V	Nombre: Antonio José Coral Triana Cargo: Gerente de riesgos y Seguridad de la información	Nombre: Antonio José Coral Triana Cargo: Gerente de riesgos y Seguridad de la información
20/02/2020	3.0	Ajustes capítulo I Para el Correo Electrónico Ajustes capítulo II Para la Gestión de Accesos Inclusión nuevo Capítulo XIV Firma Electrónica y Digital	Nombre: Marysol Kattah Cargo: Profesional Máster V	Nombre: Antonio José Coral Triana Cargo: Gerente de riesgos y Seguridad de la información	Nombre: Antonio José Coral Triana Cargo: Gerente de riesgos y Seguridad de la

FECHA	VERSIÓN	MODIFICACIÓN	ELABORÓ	REVISÓ.	APROBÓ.
		Ajustes Capítulo Capitulo VIII Para el Desarrollo Seguro			información
15/10/2021	4.0	Inclusión nuevos Capítulos (para las firmas de Colpensiones, Capítulo para las tecnologías en la nube retiro de activos de información	Nombre: Marysol Kattah Cargo: Profesional Máster V	Nombre: Antonio José Coral Triana Cargo: Gerente de riesgos y Seguridad de la información	Nombre: Antonio José Coral Triana Cargo: Gerente de riesgos y Seguridad de la información
26/01/2022	5.0	Se realizan ajustes a las políticas de seguridad con acompañamiento de la consultoría Colombia Digital donde se realizan ajustes: • capítulo para el correo electrónico es alineado a la política de "seguridad en las comunicaciones digitales" • Se crea políticas: • Política Cumplimiento de Seguridad de la Información	Nombre: Stiven Parra Córdoba Cargo: Profesional Máster VIII	Nombre: Antonio José Coral Triana Cargo: Gerente de Riesgos y Seguridad de la Información	Nombre: Fabián Mauricio Arias Cargo: vicepresidente de Seguridad y Riesgos Empresariales

FECHA	VERSIÓN	MODIFICACIÓN	ELABORÓ	REVISÓ.	APROBÓ.
		• Política de Trabajo en casa • Política de uso aceptable de activos de información • Se adicionan nuevas definiciones			
28/04/2023	6.0	• Se hace referencia a la política general de seguridad de la información y ciberseguridad • Se indica la periodicidad de revisión y actualización de este documento • Se incluye política para acceso a las redes	Nombre: Stiven Parra Córdoba Cargo: Profesional Máster, Código 320, Grado 08 Nombre: Liliana Serrano Forero Cargo: Asesor, Código 200, Grado 01	Nombre: Paola Palmariny Peñaranda, Vicepresidente de Seguridad y Riesgos Empresariales Nombre: Antonio José Coral Triana, Gerente de Riesgos y Seguridad de la Información	Nombre: Junta Directiva abril de 2023 Acuerdo 004 de 2023