POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Introducción

El Consejo Directivo del COLEGIO COLOMBIANO DE PSICÓLOGOS, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Programa de gestión de seguridad de Datos Personales, por medio de la adopción de políticas, normas y procedimientos, generando confianza en el ejercicio de sus funciones respecto del Estado, particulares, y demás interesados en el cumplimiento de las leyes, aspecto que se encuentra de la mano de la misión y visión de la Entidad.

Así, al proteger la información, se disminuye, de manera sistemática, los posibles impactos y riesgos sobre sus activos informáticos, manteniendo bajos niveles de exposición respecto de las condiciones de integridad, confidencialidad y disponibilidad de los datos personales y la información que maneja la Entidad, atendiendo los intereses de las personas que tienen algún tipo de relación con la Organización.

Se ha definido que las políticas de seguridad de la información deben identificar responsabilidades y establecer los objetivos para una protección apropiada de los activos informáticos de nuestra entidad, reduciendo el riesgo de que en forma accidental o intencional se obtengan accesos no autorizados, o se afecten las condiciones de integridad, disponibilidad y confidencialidad de la información almacenada en las bases de datos del Colegio.

2. Objetivos

2.1. Objetivo general

Establecer los lineamientos que permitan proteger los activos de información del Colegio Colombiano De Psicólogos, teniendo en cuenta los procesos y la operación de la entidad, garantizando las condiciones de confidencialidad, integridad y disponibilidad de la información almacenada, tanto a nivel digital como a nivel físico.

2.2. Objetivos específicos

- **Proteger la información:** Resguardar de manera efectiva la información, documentos y datos personales para asegurar su confidencialidad y disponibilidad.
- **Asegurar el funcionamiento de los sistemas:** Garantizar que todos los equipos y plataformas operen de manera óptima y continua.
- **Establecer políticas y procedimientos**: Generar y mantener documentación guía para la implementación y el mantenimiento del sistema de seguridad de la información, que se adapte a las necesidades del negocio y cumpla con los requerimientos regulatorios.

3. Justificación

Atendiendo a los altos flujos de información que incluyen datos personales e información de carácter confidencial que se maneja al interior del Colegio Colombiano De Psicólogos, se hace necesario garantizar unos adecuados niveles de seguridad en el tratamiento de dichos datos e información, en desarrollo del principio de responsabilidad incluido en el Decreto 1377 de 2013 y la norma ISO 27001:2022.

4. Alcance

La presente política de seguridad de la información va dirigida a Directores, Presidentes, Empleados, Contratistas, Proveedores, y, en general, hacía todos los estamentos que tengan algún tipo de relación con el Colegio Colombiano De Psicólogos, o que participen en los procesos que involucren información confidencial o datos personales sujetos a confidencialidad, y es aplicable a todo el ciclo de vida de los activos informáticos de la entidad, desde su creación, pasando por su distribución y almacenamiento, hasta su destrucción.

5. Marco regulatorio y normativo

El Colegio Colombiano De Psicólogos, al ser una entidad con funciones públicas, cuenta con un amplio margen normativo que direcciona sus prácticas en materia de gestión de seguridad de la información, entre las cuales se destacan:

- Ley 1581 de 2012.
- Decreto 1377 de 2013.
- Decreto 1266 de 2008.
- NTC-ISO 27001:2022.

Igualmente, se tendrán en cuenta e incluirán leyes, decretos, resoluciones y demás normas que complementen en el futuro el marco normativo de protección de datos personales y seguridad de la información.

6. Principios de seguridad de la información

Por medio de la presente política, se adoptan 12 principios de seguridad que soportan el Sistema de Gestión de Seguridad en la Información del Colegio, aspecto que tendrá un alto impacto en la protección de los datos personales y demás información que maneja la entidad.

6.1. Las responsabilidades frente a la seguridad de la información serán compartidas, publicadas y aceptadas por empleados, proveedores, y demás terceros que puedan tener algún tipo de acceso a esta.

6.2. Se protegerá la información generada, procesada o resguardada por cada una de sus áreas y procesos, con base en una infraestructura tecnológica que permita restringir los accesos no autorizados a la información que reposa en nuestras bases de datos.

6.3. Se protegerá la información creada, procesada, transmitida o resguardada por cada una de las áreas y procesos, para efectos de disminuir impactos financieros, operativos o legales, relacionados con un uso incorrecto de la información, por medio de la aplicación de controles que dependen de la calidad de responsable o encargado de tratamiento de datos personales.

6.4. La entidad protegerá la información de las amenazas que se desprendan de la interacción del personal con la información protegida.

6.5. La entidad protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta procesos en donde exista un alto o complejo flujo de información y datos personales.

6.6. La entidad implementará controles de acceso a la información, sistemas y recursos de red.

6.7. La entidad garantizará que la seguridad sea parte integral de la información que trata.

6.8. La entidad garantizará una adecuada trazabilidad de los eventos de seguridad y las debilidades asociadas con los sistemas de información, además de una mejora efectiva de su modelo de seguridad.

6.9. La entidad garantizará la disponibilidad de sus procesos y áreas, y la continuidad de su operación basada en el impacto que pueden generar eventos de seguridad o de falta de disponibilidad de la información.

6.10. La entidad garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

7. Política de seguridad de la información de COLPSIC

Se define la Política de Seguridad de la Información como la manifestación que realiza el Colegio Colombiano de Psicólogos, relacionado con la necesidad institucional de definir las bases para gestionar de manera adecuada y efectiva, la seguridad de la información, a través de las cuales se garantizará la integridad, confidencialidad y disponibilidad de sus activos de información.

7.1. Compromisos generales de la Organización

La organización asume los siguientes compromisos para proteger los activos de información de los procesos misionales:

7.1.1. La gestión de los riesgos de los activos de información teniendo en cuenta el nivel de tolerancia al riesgo de la entidad.

7.1.2. Una gestión integral de riesgos basada en la implementación de controles físicos y digitales orientados a la prevención de incidentes.

7.1.3. La implementación de políticas de seguridad de alto nivel y de políticas complementarias de la norma ISO 27001:2022, para asegurar la confidencialidad, integridad y disponibilidad de la información institucional.

7.1.4. Fomentar a la cultura y toma de conciencia entre el personal (funcionarios, contratistas y terceros) sobre la importancia de la seguridad de la información.

7.1.5. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

7.1.6. Proteger la información generada, procesada o resguardada por los procesos, su infraestructura tecnológica y activos del riesgo, frente a los accesos otorgados a terceros, o como resultado de un servicio interno en outsourcing.

7.1.7. Se mitigarán los incidentes de seguridad y privacidad de la información de manera efectiva, eficaz y eficiente, y se protegerá la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello, es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

7.1.8. Se protegerá la información de las amenazas originadas en acciones u omisiones del personal de la entidad.

7.1.9. Se generará conciencia para el cambio de la organización en todos sus niveles, para la generación de una cultura de apropiación de seguridad y privacidad en la información.

7.1.10. Se protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

7.1.11. Se controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

7.1.12. Se implementarán controles de acceso a la información, sistemas y recursos de red.

7.1.13. Se garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

7.1.14. Se garantizará a través de una adecuada gestión de eventos de seguridad y debilidades asociadas con los sistemas de información efectiva de su modelo de seguridad.

7.1.15. Se garantizará la disponibilidad de sus procesos misionales y la continuidad de su operación basada en el impacto que pueden generar los eventos.

7.1.16. Se garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

7.2. **Compromisos individuales**

Se adoptarán los siguientes deberes de los usuarios de la información, desde el punto de vista individual:

7.2.1. Usar la información del Colegio Colombiano De Psicólogos de manera exclusiva para

propósitos de la misión de la entidad y en cumplimiento de su labor.

7.2.2. Respetar la confidencialidad de la información del Colegio Colombiano De Psicólogos.

7.2.3. No compartir perfiles de usuario, contraseñas, sesiones en estaciones de trabajo, documentos o cualquier tipo de información confidencial.

7.2.4. No anotar y/o almacenar en lugares visibles contraseñas de acceso a los sistemas.

7.2.5. Ajustarse a las directrices de clasificación de la información.

7.2.6. Bloquear la sesión de la estación de trabajo al momento de ausentarse de la misma.

7.2.7. Las impresiones deben ser recogidas al momento de generarlas, no se deben dejar por largos periodos de tiempo en la impresora.

7.2.8. Devolver y no conservar ningún tipo de copia en sus activos de información, en buen estado, una vez cese su relación laboral con la entidad.

7.2.9. Está estrictamente prohibida la divulgación, retiro o pérdida no autorizada de información de la entidad almacenada en medios físicos removibles como USB, cintas magnéticas, entre otras.

7.2.10. Está estrictamente prohibida la utilización de software no licenciado en los recursos tecnológicos, copiar software licenciado del Colegio Colombiano De Psicólogos, para usar en computadores personales, ya sea en su domicilio o en cualquier otra instalación y/o entregarlos a terceros.

7.2.11. Asegurar el uso de equipos y dispositivos debidamente autorizados por el área de Tecnología, de tal forma que sean seguros para acceder a la información sensible de la organización.

7.2.12. Se debe notificar de inmediato cualquier incidente de seguridad o sospecha de brecha de datos a la persona o unidad responsable de la seguridad de la información.

7.3. **Deberes de los responsables de personal**

Adicionalmente, se mencionan a continuación los deberes de los responsables de personal:

7.3.1. Conceder autorizaciones de acceso a la información acorde con las funciones a ser realizadas por sus subordinados.

7.3.2. Hay que asegurar que los privilegios de acceso de cada empleado reflejan una adecuada distribución de funciones.

7.3.3. Restringir el acceso del personal a aquellas áreas que hayan sido restringidas por razones de seguridad.

7.3.4. Ser el responsable de conocer, solicitar y ratificar los privilegios de acceso a los empleados que le reportan.

7.3.5. Conservar los registros de los empleados con privilegios de acceso a la información.
7.3.6. Los contratos de outsourcing deben identificar los acuerdos relacionados con la propiedad de la información y la no divulgación de información confidencial.
7.3.7. Cuando un empleado se ausenta de su trabajo por un período de tiempo superior al mínimo establecido debe:
7.3.7.1 Determinar si los accesos a los recursos físicos y a la información deben ser suspendidos.
7.3.7.2 Notificar la fecha en que el acceso debe ser suspendido, de ser necesario.
7.3.7.3 Recoger los equipos de seguridad como llaves, claves, computadoras, etc.
7.3.7.4 Cuando un empleado se encuentra por fuera de sus funciones, el acceso a los recursos físicos y a la información debe ser inmediatamente suspendido.
7.3.8. Cuando un empleado es retirado voluntaria o involuntariamente, su jefe inmediato es responsable por:
7.3.8.1. Solicitar la revocación de las autorizaciones.
7.3.8.2. Revocar o restringir los privilegios de acceso antes de notificarle la terminación del contrato, si es apropiado.
7.3.8.3. Recoger los equipos, dispositivos físicos y la revocación de las autorizaciones a sistemas de información.

7.4. **Manejo de información confidencial**

Consecuentemente, se emiten las siguientes directrices relacionadas con el manejo de información confidencial:

7.4.1. Los documentos que contengan información no pueden estar almacenados de manera insegura.
7.4.2. El usuario dueño o fuente de información debe asegurar la marcación necesaria para garantizar el orden de los datos e identificación de los mismos.
7.4.3. Debe ser apropiadamente autorizado para la divulgación de acuerdo con los estándares de clasificación de la información por parte de los propietarios.
7.4.4. La divulgación cualquiera que fuere su medio, verbal, escrita, telefónica o electrónica, debe ser efectuada sobre la base de la necesidad de conocerla de acuerdo con sus funciones.
7.4.5. Las reuniones relacionadas con el manejo de la información deben llevarse a cabo en sitios cerrados.
7.4.6. No debe ser accedida a través de tecnologías de fácil acceso como cadenas de mensajería instantánea o redes sociales (Facebook, WhatsApp).
7.4.7. Para propósitos de seguridad toda la información debe ser etiquetada con la clasificación respectiva.
7.4.8. El etiquetado debe ser fácilmente leíble a simple vista.
7.4.9. Antes de divulgar verbalmente información clasificada como restringida o

confidencial, debe indicarse su clasificación.

7.4.10. El acceso o distribución de información de uso interno debe estar limitado a empleados u otros con la necesidad de conocerla o usarla para cumplir con sus funciones.

7.4.11. Los documentos que contengan información confidencial deben ser impresos en un área segura o con la supervisión adecuada.

7.4.12. La distribución de información confidencial debe ser limitada a personas o grupos con la necesidad de conocerla o usarla para cumplir sus funciones.

7.4.13. Los mecanismos de entrega utilizados para información restringida deben contemplar confirmación de recibido.

7.4.14. Estas políticas se aplican tanto a los originales como a todas las copias de la información.

7.4.15. El acceso a información confidencial que se encuentre almacenada debe ser adecuadamente controlado, incluyendo el almacenamiento externo, o de copias de respaldo.

7.4.16. Las copias de respaldo de información confidencial deben ser protegidas de destrucción intencionada o accidental.

7.4.17. La información almacenada por períodos prolongados debe ser revisada regularmente para verificar su legibilidad.

7.4.18. Las personas que trabajan desde casa o fuera de la oficina deben asegurarse de que sus dispositivos sean seguros y estén actualizados, aplicando las mismas medidas de seguridad que se requieren en el entorno de trabajo, con el apoyo y aprobación del área de Tecnología.

7.4.19. Todos los documentos y datos del Colegio Colombiano de Psicólogos deben ser almacenados en plataformas autorizadas y no deben ser guardados en dispositivos personales o en servicios de almacenamiento en la nube no aprobados.

7.4.20. Es obligatorio que las personas que trabajen desde casa o fuera de las instalaciones del Colegio, garanticen que la información esté guardada en los medios autorizados y cumpliendo los procedimientos establecidos al interior del mismo.

7.4.21. Todos aquellos que cuenten con acceso remoto a la información del Colegio Colombiano de Psicólogos son responsables por la seguridad de la información con los mismos niveles de control que se tienen al interior de la entidad.

7.5. **Disposiciones sobre el uso adecuado de software**

7.5.1. En los puestos de trabajo del Colegio Colombiano De Psicólogos, sólo se pueden instalar software desarrollado o adquirido legalmente y cuya licencia de uso esté a nombre de la entidad evitando riesgos de seguridad asociados con software no autorizado.

7.5.2. La coordinación y ejecución de mantenimiento de los equipos de cómputo y de trabajo, deberá ser gestionada exclusivamente por personas pertenecientes al Colegio.

7.5.3. Los usuarios deben cumplir con la normatividad relacionada con los derechos de autor.

7.6. **Disposiciones sobre el control de virus**

7.6.1. Los computadores personales deben mantener activo un software antivirus de manera obligatoria, un sistema operativo, acceso a Microsoft office, licenciados y actualizados, con su debida autorización del equipo de tecnología.

7.6.2. Los servidores de archivos, groupware y correo electrónico deben mantener activo un software antivirus.

7.6.3. Los computadores y servidores personales que estén autorizados por tecnología deben ser analizados contra virus de manera periódica y automática.

7.6.4. Cualquier información que venga por medio electrónico o magnético como correo electrónico o información de internet, debe ser revisada por un software antivirus antes de ser descargada y utilizada.

7.6.5. El equipo de trabajo del área de tecnología es responsable de la actualización oportuna del software antivirus.

7.6.6. Es responsabilidad de los usuarios reportar los incidentes de infección o sospecha de virus a las áreas encargadas.

7.6.7. Es responsabilidad de los usuarios mantener toda la información en los repositorios autorizados por tecnología y verificar que los archivos o documentos que se carguen estén libres de cualquier infección de virus.

7.6.8. El usuario debe asegurar que toda la información provenga de fuentes conocidas.

7.6.9. Ningún usuario puede escribir, distribuir o introducir software que conozca o sospeche que tiene virus.

7.7. **Control de Contraseñas**

7.7.1. Los perfiles de usuario y la contraseña tienen que ser asignados de manera individual, generando responsabilidad por el uso de dichas credenciales de acceso.

7.7.2. Los usuarios no pueden prestar su contraseña, lo que se realice con su perfil queda bajo la responsabilidad de su titular.

7.7.3. El usuario no debe compartir, escribir o revelar su contraseña.

7.7.4. Las contraseñas individuales no deben ser mostradas en texto claro. Todos los sistemas de procesamiento deben eliminar la visualización de contraseñas ya sea en pantallas o en impresoras.

7.7.5. Las contraseñas deben cambiarse en un periodo máximo de 90 a 120 días, esto será configurado de manera regular y automática por el área de Tecnología.

7.7.6. Si un sistema no obliga al cambio de contraseña, es responsabilidad del usuario realizar este cambio.

7.7.7. No se deben repetir contraseñas utilizadas anteriormente, en los últimos cinco cambios.

7.7.8. Debe verificarse la identidad del usuario antes de que las contraseñas o perfiles de usuario sean habilitados nuevamente. Solo se puede cambiar una contraseña cuando el perfil de usuario pertenezca a quien solicita el cambio.

7.7.9. La identificación del usuario y su contraseña no deben ser iguales.

7.7.10. Las contraseñas deben ser cuidadosamente seleccionadas para que no sean adivinadas fácilmente, por ende:

a. No se debe utilizar algún nombre, apellidos, ni propios o de familiares.
b. No se debe utilizar información fácil de obtener como placa o marca del carro, número de teléfono, marca, nombre del edificio.
c. No deben usarse contraseñas sólo numéricas o alfanuméricas.
d. Use contraseñas fáciles de recordar para que no tenga que escribirlas.
e. No use el nombre de perfil de usuario en ninguna forma (duplicado o reversado).

7.7.11. Siempre que el administrador de contraseñas asigne una contraseña, es responsabilidad del usuario cambiarla en su primer uso.

7.8. **Copias de respaldo de información (Backups)**

7.8.1. Se debe contar con un sistema automático para la recolección de copias de respaldo.

7.8.2. Las copias de respaldo deben tener el mismo nivel de protección de la información que poseen en su fuente original.

7.8.3. Los medios magnéticos que contienen información deben ser almacenados en lugares físicamente seguros.

7.8.4. Los usuarios son responsables de almacenar la información en los espacios físicos y/o digitales designadas por la Dirección de Tecnología y por los directores encargados de la gestión de la información. Además, deberán proporcionar apoyo oportuno para las pruebas de restauración de dicha información.

7.8.5. Se llevarán a cabo pruebas periódicas de restauración de información en las diferentes áreas, conforme a lo establecido por la Dirección de Tecnología, con el fin de garantizar la integridad de los datos y de los sistemas de información.

7.8.6. Los medios magnéticos deben tener rótulos visibles y legibles tanto internos como externos.

7.8.7. Se debe mantener suficientes respaldos de la información para que en caso de contingencia se pueda recuperar la información oportuna.

7.8.8. Para responder adecuadamente a una contingencia, los respaldos de la información

se deben almacenar en sitios externos.

7.8.9. Cualquier medio magnético que contenga información clasificada como restringida o confidencial debe estar identificada.

7.8.10. Al enviar información clasificada como restringida o confidencial a terceros se debe exigir un acuse de recibo.

7.8.11. Todos los medios que contengan información clasificada como restringida o confidencial y que finalice su ciclo de vida, deben ser sobre escritos o destruidos físicamente para que la información no pueda ser recuperada.

7.8.12. Es responsabilidad de los administradores de las plataformas, mantener el respaldo de la configuración del sistema operativo y de los servicios que éstas proveen.

7.9. **Navegación de Internet – Filtrado Web - Prevención Fuga de información**

Con el fin de salvaguardar la integridad y seguridad de la información dentro de la organización, se implementarán reglas y controles restrictivos en la navegación de internet. Estas directrices están diseñadas para todos los usuarios que acceden a la red interna y utilizan los equipos de cómputo asignados por Colpsic.

Los sitios web se clasificarán en categorías de navegación para facilitar un control de acceso más efectivo.

7.9.1. Restricciones de navegación a sitios web, categorías de contenido sexual, violencia y actividades criminales, juegos de azar y apuestas, uso de drogas, descarga de software y sitios similares que puedan afectar la seguridad de la información.

7.9.2. Restricciones de navegación a categoría streaming y sitios de entretenimiento web.

7.9.3. Restricciones de navegación a categorías de almacenamiento nube, Dropbox, mega, entre otros similares, para garantizar el acceso único a sitios aprobados por la dirección ejecutiva y dirección de tecnología del Colegio Colombiano de Psicólogos - Colpsic.

7.9.4. Restricciones de unidades extraíbles como discos duros, USB, Dispositivos MTP, que no estén autorizados por la dirección de tecnología o dirección Ejecutiva de Colpsic.

7.9.5. Restricciones de acceso a espacios de almacenamiento de información física y confidencial que serán autorizados por cada director de área o por la dirección ejecutiva.

7.10. **Acceso a áreas restringidas**

Políticas de seguridad en el acceso a áreas restringidas:

7.10.1. El acceso a las áreas donde se procesa y almacena información del Colegio Colombiano De Psicólogos clasificada como restringida o confidencial debe ser autorizado a aquellos empleados con necesidades de acceso.

7.10.2. Los servidores de aplicaciones y bases de datos, y otros dispositivos, que son utilizadas para mantener funciones críticas del negocio, deben estar en un área de acceso restringido y separadas del ambiente de las oficinas.

7.10.3. Las puertas exteriores deben ser cerradas con llave o estar aseguradas en horas no hábiles.

7.10.4. Las áreas diseñadas como restringidas deben tener controles de acceso especiales, y solo podrá acceder el personal autorizado.

7.10.5. Los privilegios de acceso físico autorizados deben ser convalidados periódicamente por los jefes de áreas, secretarios, directores, subdirectores, gerentes y demás personas designadas para tal fin, e igualmente deberán ser restringidos, modificados o revocados oportunamente a la terminación, transferencia o cambio en las funciones de una empresa.

7.10.6. Los jefes, directores, subdirectores, gerentes, secretarios y demás personas designadas para tal fin, y los encargados de áreas de acceso restringido deben asegurar que los controles de acceso como llaves de seguridad o cerraduras con llaves maestras sean cambiadas cuando el control haya sido comprometido.

7.10.7. Las cerraduras convencionales deben ser cambiadas periódicamente.

7.10.8. Se debe restringir el ingreso de dispositivos móviles a áreas catalogadas como restringidas.

7.11. **Manejo de documentos electrónicos**

7.11.1. Los usuarios deben tratar los mensajes de correo electrónico y archivos como información de propiedad del Colegio Colombiano De Psicólogos.

7.11.2. Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera comprimida y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de funciones y atribuciones.

7.11.3. Las comunicaciones electrónicas en lo posible deben ser concretas, precisas y completas.

7.11.4. Las comunicaciones electrónicas oficiales hacia el exterior deben ser revisadas por un jefe inmediato, puede ser un coordinador de área, líder, subsecretario o secretario; sin este requisito, no serán consideradas como documentos oficiales

del Colegio Colombiano De Psicólogos.

7.11.5. Solamente se considera oficial un mensaje de correo electrónico que incluya el nombre y cargo del funcionario de la dependencia de donde se envía.

7.11.6. Las comunicaciones oficiales y circulares del Colegio Colombiano De Psicólogos deben ser escaneadas y enviadas desde el correo electrónico de quien las elabora al funcionario autorizado para manejar la cuenta de comunicados generales.

7.11.7. Los comunicados generales son comunicados emanados desde la administración central hacia la totalidad de los funcionarios; los cuales únicamente deben ser enviados por un funcionario de la Dirección Ejecutiva Nacional o la Dirección de Comunicaciones. El funcionario autorizado es quien realizará el filtro de los correos de interés general para luego ser enviados a la comunidad general que se necesite. Además, no puede enviarse información con logotipos o propaganda de índole política, comercial o sindical.

7.11.8. Se deben conservar los niveles de seguridad en el manejo de la información electrónica.

7.11.9. La asignación de cuentas de correo electrónico a contratistas será autorizada por el equipo de tecnología.

7.11.10. Todas las direcciones de correo electrónico deben ser creadas usando el estándar definido por la entidad.

7.11.11. Todos los funcionarios del Colegio Colombiano De Psicólogos tendrán correo electrónico personalizado, si así lo requieren.

7.11.12. El uso del correo electrónico para fines personales está prohibido. Las herramientas asignadas deben ser usadas únicamente con fines corporativos.

7.11.13. Se establecerá un tamaño de buzón de correo para cada usuario, es decir, un espacio en disco en el servidor de correo, destinado al almacenamiento de mensajes electrónicos de cada usuario.

7.11.14. El usuario responsable del buzón deberá dar un trámite ágil al correo electrónico recibido, es decir, diariamente debe leer, responder y eliminar o archivar en el disco duro local, solamente los mensajes que soporten información relevante para el desarrollo de sus labores en la entidad.

7.11.15. El mantenimiento de la lista de contactos y del buzón será responsabilidad del usuario y deberá conservar únicamente los mensajes necesarios para no exceder el máximo límite de almacenamiento.

7.11.16. Los mensajes deben ser redactados de forma clara y concreta, evitando el uso de mayúsculas sostenidas, que, según normas internacionales de redacción en internet, equivale a gritar.

7.11.17. En el nombre del destinatario y el asunto debe evitarse el uso de caracteres especiales como slash (/), tildes (‘), guiones (-), etc.

7.11.18. Los mensajes de correo salientes siempre deben llevar en el campo “Asunto” una frase que haga referencia directa al contenido del texto.

7.11.19. Todos los mensajes de correo enviados deben contener como mínimo la

siguiente información: Nombre: Cargo: Dependencia: Entidad: Teléfono: Ext. Email.

7.11.20. Ningún usuario deberá permitir a otro enviar correos utilizando su cuenta sin aclarar el remitente.

7.11.21. Cuando un funcionario requiere ausentarse de la entidad por un período superior a 8 días debe programar el correo electrónico para que automáticamente responda a los remitentes indicando fecha de llegada, nombre y dirección de correo electrónico de la persona encargada durante su ausencia.

7.11.22. Antes de enviar un correo deberá verificarse que esté dirigido solamente a los interesados y/o a quienes deban conocer o decidir sobre el tema, evitando duplicidades o desmejoramiento en el servicio y operación de la red.

7.11.23. Los usuarios deben cerrar sesión en su cuenta de correo electrónico inmediatamente después de usarla desde un lugar externo a las oficinas, para prevenir el acceso no autorizado a la información sensible.

7.11.24. En caso de pérdida o robo de dispositivos que contengan acceso a la cuenta de correo electrónico, los usuarios deben reportar inmediatamente el incidente para bloquear los accesos y proteger la información.

7.12. Contratación de los servicios de un tercero encargado del tratamiento de bases de datos

7.12.1. Colpsic debe asegurarse de que cualquier tercero cumpla con la regulación de protección de datos personales y que sus políticas al respecto se encuentren en línea con las establecidas por COLPSIC. En este sentido, los siguientes son los aspectos para tener en cuenta al momento de contratar un encargado:

7.12.2. Que cuente con una Política de Tratamiento de Datos.

7.12.3. Que disponga de una canal oficial para la atención de consultas y reclamos.

7.12.4. Que las actividades que el tercero va a desarrollar se enmarcan en la autorización del titular de los datos.

7.12.5. Que cuenta con mecanismos técnicos, humanos y administrativos para garantizar la seguridad de la información.

7.12.6. Que terminado el servicio devolverá (destruirá) la información que le fue entregada.

7.12.7. Tener en cuenta que responderá por el uso indebido o no autorizado de la información personal que le fue entregada.

7.12.8. Es recomendable que en los contratos de prestación de servicios celebrados con terceros se establezcan de manera clara las obligaciones especiales y los deberes que deben cumplir los encargados en el tratamiento de datos personales. Así mismo, es fundamental que, como mínimo, se pacten cláusulas contractuales en las que se obliguen a:

7.12.9. Cumplir las políticas de tratamiento de información de Colpsic.

7.12.10. Garantizar seguridad y confidencialidad de los datos personales.

7.12.11. No usar los datos personales para fines diferentes a los autorizados o no acceder a los mismos (según el caso).
7.12.12. No apropiarse de los datos personales (copias de planillas, formularios, grabaciones, archivos electrónicos) luego de culminado el contrato de prestación de servicios.
7.12.13. Devolver a Colpsic todos los datos que trató durante la prestación de sus servicios.

8. Organigrama de implementación, modificación y actualización de la presente política de seguridad

Esta sección define los roles y responsabilidades en cuanto a la implementación de la seguridad de la información y datos personales. Esta política aplica a todos los implicados en la operación de la entidad, teniendo en cuenta que cada uno cumple un rol en el manejo y administración de la seguridad de la información.

La presente política debe ser revisada mínimo una vez cada dos años, o cuando se produzca un cambio relevante en la operación que implique realizar ajustes o producto de los cambios en el entorno tecnológico y/o de las necesidades de la operación de la entidad.

A continuación, se relacionan las responsabilidades en cuanto a seguridad de la información y el tratamiento adecuado de datos personales:

8.1. Apoyo de la Alta Dirección

Las Directivas del Colegio Colombiano De Psicólogos deben apoyar activamente la seguridad de la información dentro de la entidad, definir un rumbo claro, en desarrollo del principio de responsabilidad demostrada, junto con el conocimiento de las responsabilidades en materia de seguridad de la información:

8.1.1. El Colegio Colombiano De Psicólogos debe mantener dentro de sus colaboradores dos colaboradores un con el rol de Oficial de Protección de Datos Personales y otro con el rol de Oficial de Seguridad de la Información, quienes serán los encargados de realizar el debido tratamiento de datos y la aplicación de los lineamientos de seguridad información.
8.1.2. Se debe velar por el cumplimiento y aplicación de la política de seguridad de la información y las normas relacionadas, por parte de todos los funcionarios y partes interesadas del Colegio.
8.1.3. Se debe identificar y asignar responsabilidades a las áreas y personas que trabajen en alguna fase del ciclo de vida de la información que reposa en las bases de datos del Colegio.
8.1.4. La alta dirección del Colegio Colombiano De Psicólogos debe apoyar, facilitar y mantener cuando se requiera relaciones con empresas, entidades u organismos

que presten asesoría especializada en seguridad de la información. Se deben establecer tres niveles diferentes de gestión de seguridad de la información, en la participación de la definición y aplicación del Sistema de Gestión de Seguridad de la Información (SGSI):

8.1.4.1. **Estratégico:** Dirigir y proveer: Definir los grandes lineamientos directivos o gerenciales para la seguridad de la información y la política global del SGSI. De igual manera coordinar y aprobar los recursos.

8.1.4.2. **Táctico:** Implementar y optimizar: Diseñar e implementar el SGSI, establecer objetivos concretos o específicos y gestionar los recursos asignados.

8.1.4.3. **Operacional:** Ejecutar y reportar: Alcanzar los objetivos específicos mediante procesos técnicos.

8.2. **Oficiales de protección de datos personales y seguridad de la información**

Los oficiales de Protección de Datos Personales y Seguridad de la Información deben desarrollar todas las actividades relacionadas con la gestión de Protección de Datos Personales y Seguridad de la Información.

8.2.1. Implementación de las Políticas de Seguridad de Información y Tratamiento de Datos Personales, junto con los diferentes documentos soporte relacionados (Protocolos, instructivos, lineamientos, entre otros).

8.2.2. Generación de formatos o herramientas que permitan el cumplimiento de la normatividad en las diferentes actividades.

8.2.3. Preparación de la entidad para el cumplimiento de la norma ISO 27001:2022, ley 1581 de 2012 y demás normas o decretos reglamentarios que apliquen.

8.2.4. Revisar, proyectar y proponer modificaciones de la presente política, según sea requerido.

8.2.5. Mantener trazabilidad sobre las evaluaciones de impacto y de amenazas a seguridad informática de la entidad.

8.2.6. Realizar las actividades de formación y recordación de los lineamientos establecidos para el cumplimiento de las políticas establecidas.

8.2.7. Revisar y adoptar protocolos de respuesta en el manejo de violaciones e incidentes de seguridad, para implementar mejores prácticas o recomendaciones y lecciones aprendidas de revisiones posteriores a esos incidentes.

8.2.8. Revisar y modificar los requisitos mínimos solicitados en relación con los encargados del tratamiento.

8.2.9. Actualizar y aclarar las comunicaciones externas para explicar las políticas de tratamiento de datos y de seguridad de la información, con apoyo en las áreas encargadas.

8.2.10. Servir de enlace y coordinación con las demás áreas de la organización para asegurar una implementación transversal de los lineamientos y políticas

relacionados con la Protección de Datos Personales y Seguridad de la Información.

8.2.11. Obtener las declaraciones de conformidad ante la Superintendencia de Industria y Comercio (SIC) cuando sea requerido según la normativa vigente.

8.2.12. Registrar las bases de datos de la organización en el registro nacional de bases de datos y actualizar el reporte según los requerimientos de la SIC.

8.2.13. Analizar las responsabilidades de cada cargo respecto a la protección de datos personales de la organización.

8.2.14. Medir la participación y evaluar el desempeño en los espacios de formación referentes a protección de datos y seguridad de la información.

8.2.15. Capacitar a los empleados que tengan acceso a datos personales e información gestionada por la organización.

8.2.16. Evaluar, apoyar, dar visto bueno y emitir conceptos técnicos, sobre nuevas soluciones o plataformas tecnológicas a adquirir o implementar en el Colegio Colombiano De Psicólogos.

8.2.17. Crear y revisar los acuerdos de confidencialidad con funcionarios, contratistas, proveedores y terceros.

8.2.18. Verificar la aceptación y aprobación de riesgos identificados, y de sus planes de tratamiento.

8.2.19. Revisar y actualizar periódicamente los inventarios de activos de información, definiendo responsabilidades de criticidad, sensibilidad, reserva, protección adecuada e infraestructuras.

8.3. **Todas las dependencias y oficinas del Colegio Colombiano de Psicólogos**

Todos los empleados, dependencias, contratistas y oficinas del Colegio Colombiano De Psicólogos deberán tener en cuenta los siguientes lineamientos:

8.3.1. Toda adquisición de una solución o plataforma tecnológica debe contar con el visto bueno, concepto técnico y acompañamiento del equipo de tecnología en donde se evalúen los aspectos de viabilidad técnica al momento previo de la realización de la solicitud o confirmación de compra. Esto validando compatibilidad, capacidad, integridad y disponibilidad, tanto desde la óptica de infraestructura de la Dirección de Tecnología, como de seguridad de la información.

8.3.2. Todo requerimiento, incidente, problema o cambio debe ser reportado y tramitado por medio de la Dirección de tecnología y el Oficial de Protección de Datos Personales, único medio válido y autorizado para estos fines.

8.3.3. El personal del equipo de tecnología está autorizado para realizar o supervisar el mantenimiento, cambios de partes, cambio de aplicativos, y/u otra actividad que genere modificaciones que afecten la seguridad en los equipos de propiedad del

Colegio Colombiano De Psicólogos.

8.3.4. Incluir y tener en cuenta los lineamientos y políticas de seguridad de la información en la gestión de la contratación con terceros, proveedores y contratistas, así como en la gestión de proyectos, independientemente del tipo de proyecto.

8.3.5. Cumplir y apoyar el cumplimiento de todas las políticas, normas, manuales y procedimientos y otros que correspondan de seguridad de la información.

8.4. Funcionarios - contratistas del Colegio Colombiano de Psicólogos

Los usuarios de la información (funcionarios – contratistas - proveedores - terceros) y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer y cumplir la Política de Seguridad de la Información vigente. Los funcionarios, contratistas, proveedores, terceros del Colegio Colombiano De Psicólogos, deben:

8.4.1. Conocer, comprender y aplicar la Política de Seguridad de la información del Colegio Colombiano De Psicólogos en los procedimientos que apliquen a su trabajo.

8.4.2. Llevar a cabo su trabajo, asegurándose de que sus acciones no producen ninguna infracción de seguridad de la información.

8.4.3. Comunicar las incidencias de seguridad de la información que detecte a los Oficiales de datos seguridad de la Información y Protección de datos personales.

8.4.4. Hacer uso de las mejores prácticas definidas en la entidad para todos los temas relacionados con la seguridad de la información.

8.4.5. Cumplir con el acuerdo de confidencialidad firmado con la entidad.

8.4.6. Reportar a los Oficiales de Protección de Datos Personales y Seguridad de la Información cualquier anormalidad que atente contra la seguridad de la información en la entidad.

9. Revisión de las presentes políticas de seguridad en la información

La Alta Dirección, junto con el Oficial de Protección de Datos Personales, deben revisar las Políticas de Seguridad en la Información del Colegio Colombiano De Psicólogos para asegurar su conveniencia, suficiencia y eficacia. Esta revisión debe incluir la evaluación de oportunidades de mejora y la necesidad de cambios del Sistema de Gestión de Seguridad de la Información y Protección de Datos Personales, incluidos la política de protección de datos personales y la política de seguridad de la información. Los resultados de dichas revisiones se deben documentar claramente y se deben llevar registros.

De la misma manera, una vez implementada la presente Política de Seguridad en la Información, normas, procedimientos, estándares, controles, formatos y procedimientos, deben ser revisados y actualizados sistemáticamente, de forma periódica y planificada (mínimo una vez por periodo o cada vez que ocurra un cambio sustancial en los activos de información), esto por parte del Oficial de

Protección de Datos Personales, el oficial de Seguridad de la Información y el Comité de Calidad del Colegio.

En su defecto, si se requiere una certificación y revisión independiente, se debe realizar por un organismo, empresa o consultor externo especializado. En cuyo caso debe seguir los lineamientos de las normas vigentes.