La presente política, regula las condiciones generales de la seguridad de la información de PROCONVET S.A., con NIT. 830.119.043-0

CAPÍTULO I
GENERALIDADES

ARTÍCULO 1. Objetivo. Con el fin de dar cumplimiento a lo establecido por la Ley 1581 de 2012 y su decreto reglamentario número 1377 de 2013, PROCONVET S.A. delega para la seguridad de su información al área de sistemas, quien es la encargada de administrar el sistema de información que hace uso la compañía, además de ofrecer servicios de red a todos los usuarios. Por lo anterior se hace necesario emitir la presente Política de Seguridad.

ARTÍCULO 2. Propósito de la Política. El propósito de esta política es ayudar a minimizar el riesgo de daño o pérdida de la información por incidentes o actividades de delincuentes, las cuales también pueden afectar los servicios de la red. Para lo cual se establecen normas que permitan lograr una adecuada protección de la información, incluyendo las reglas de comportamiento de los usuarios y administradores del sistema de la red. Por medio de esta política se busca autorizar al personal encargado, de monitorear la red local con el fin de prevenir cualquier mal uso e investigar incidentes de seguridad que se presenten.

ARTÍCULO 3. Alcance de la Política. La presente Política establece las normas para la seguridad de la información en la red de datos administrada por el área de sistemas, la cual afecta a todos los empleados y demás usuarios finales que hacen uso de los recursos informáticos de la PROCONVET S.A., quienes a partir de este momento se llamarán USUARIOS.

ARTÍCULO 4. Responsabilidades. El área de sistemas es la responsable de socializar la Política de Seguridad entre quienes hagan uso de los sistemas de información de PROCONVET S.A. De acuerdo con el perfil del usuario, se dará a conocer la Política completa. Es responsabilidad de cada usuario cumplir con cada una de las directrices que se definan en esta Política de Seguridad.

ARTÍCULO 5. Definiciones. Las siguientes definiciones son dadas con el fin de aclarar algunos conceptos para el conocimiento de la presente política:

1. Información confidencial de la organización: Es toda información relacionada con la organización que, en caso de robo o pérdida, pueda generar daños o problemas de continuidad para la PROCONVET S.A.
2. Sistema informático: Conjunto de hardware y software con el que cuenta la organización.
3. Sistema de información: Es un conjunto de elementos (información, personas y recursos) que interactúan entre sí para procesar la información y distribuirla de manera adecuada dentro de la PROCONVET S.A.

CAPÍTULO II.
USO DEL CORREO ELECTRÓNICO E INTERNET

ARTÍCULO 6. Uso del Correo Electrónico e Internet. El correo electrónico no debe ser utilizado para transmitir información confidencial de la PROCONVET S.A. En caso de que exista la necesidad de usar este medio para tal fin, se recomienda utilizar mecanismos como el cifrado para proteger la información de personas no autorizadas.

El correo electrónico debe ser de uso personal, cada usuario se hace responsable de asignar una contraseña segura y de hacer el uso correcto de éste.

El correo electrónico ni la Internet deben ser usados para publicar propaganda política, ni mensajes racistas, ni contenido sexual y ningún otro contenido que pueda afectar negativamente a los usuarios de dichos servicios.

El servicio de la Internet debe ser utilizado únicamente como un medio de consulta para fines laborales o para el cumplimiento de los objetivos organizacionales.

El área de sistemas deberá incentivar el buen uso de Internet, evitando que se haga uso indebido y malintencionado de Internet y de los servicios que sobre éste se brindan.

ARTÍCULO 7. Administración de Cuentas de Usuario. Se debe definir claramente los perfiles de usuario de acuerdo con las funciones, roles que desempeña y de su tipo de vinculación dentro de la PROCONVET S.A. De acuerdo con esto los usuarios tendrán los permisos correspondientes para realizar determinadas modificaciones (Ej.: instalación de software en computadores personales) en los distintos sistemas informáticos.

El área de sistemas es la responsable de definir los perfiles de usuario y la única de crear las cuentas de usuario teniendo en cuenta los perfiles ya definidos.

ARTÍCULO 8. Autenticación. El acceso a los servicios o sistemas que manejen información confidencial de la PROCONVET S.A., obligatoriamente, debe incluir un mecanismo de autenticación.

Todos los servicios informáticos deberían incluir autenticación de usuario, como contraseñas, certificados u otros mecanismos como doble factor de autenticación.

Se deberán establecer reglas para el uso de contraseñas seguras, como sólo permitir contraseñas que incluyan caracteres alfanuméricos y especiales dentro de la contraseña o cantidades mínimas de caracteres en la contraseña.

Los usuarios y contraseñas para acceder a los distintos servicios, computadoras y demás sistemas informáticos son personales y no deben compartirse con otros usuarios.

Las contraseñas deben ser memorizadas, y no se debe recurrir a la práctica de escribirlas en papeles ni en otro medio al cual puedan acceder otros usuarios.

El responsable del equipo no debe otorgar acceso al equipo a otras personas sin autorización del área de sistemas.

ARTÍCULO 9. Control de Acceso. El acceso a las áreas que contengan sistemas con información confidencial (Ej.: servidores) o permitan acceso privilegiado a la red (Ej.: switch) deberá ser registrado con la fecha, hora de entrada y salida, y motivo de la visita.

La visita de personas que no pertenezcan a el área de sistemas a los cuartos de servidores y equipos deberá ser bajo supervisión del personal de El área de sistemas o una persona delegada para tal fin.

Se deberá generar mecanismos que restrinjan el acceso a personas no autorizadas a las áreas que contengan sistemas con información confidencial o permitan acceso privilegiado a la red de acuerdo con el nivel de criticidad del área.

Se deben tener mecanismos que no permitan el acceso a los servidores por usuarios no autorizados.

Se deben establecer diferentes zonas lógicas en la red, en las que se separen los recursos de acceso público con los de acceso privado, filtrando tráfico de la red entre las dichas zonas.

ARTÍCULO 10. Autorización de Acceso a la información y Sistemas. Se deben definir los diferentes niveles de autorización para los usuarios de acuerdo con sus roles dentro de la PROCONVET S.A.

La autorización para acceder a la información de la PROCONVET S.A. y sistemas debe sólo ser concedida de acuerdo con el nivel requerido por el rol del usuario.

La autorización para acceder a la información y sistemas debe ser verificada como mínimo en periodos de un año.

CAPÍTULO III.
SEGURIDAD FÍSICA

ARTÍCULO 11. Seguridad física. Los equipos que procesen información sensible o crítica deben ser ubicados en lugares seguros, que tengan un perímetro de seguridad física definido y donde existan controles de acceso.

Los equipos de red deberán ser ubicados en lugares que cumplan con los requerimientos básicos de seguridad exigidos por el área de Informática. Se deberá implementar mecanismos para protección contra incendio, tales como detectores de humo, extintores de fuego o los que se consideren necesarios.

Se debe evitar almacenar material combustible o que pueda ayudar a la propagación de un incendio en los cuartos con equipos que manejen información sensible o sean de gran importancia para el funcionamiento de la red.

Es recomendable el monitoreo de las condiciones ambientales, tales como temperatura, con el fin de controlar las condiciones que puedan afectar el funcionamiento de los equipos.

ARTÍCULO 12. Software. En los equipos se deberán mantener actualizado aquel software del que se emita una mejora en seguridad o cualquiera que contribuya con el buen funcionamiento de éste.

En los equipos que manejen información sensible se deberá instalar la actualización del software garantizando que ésta no afecte con el funcionamiento del equipo.

El software instalado en los equipos debe cumplir con el licenciamiento apropiado y acorde a la propiedad intelectual a que dé lugar.

En los sistemas críticos se debería planear la actualización del software, el cual es recomendable realizar bajo un procedimiento de instalación emitido por el área de Informática.

Todo software que afecte la integridad y rendimiento de los recursos de la red no debe ser permitido.

Corresponde a El área de sistemas la autorización de la adquisición del software.

El área de sistemas es la responsable de llevar a cabo revisiones a los sistemas informáticos propiedad de la PROCONVET S.A. con el fin de asegurar que sólo software licenciado se encuentre instalado en ellos.

El software utilizado en la PROCONVET S.A. deberá ser usado exclusivamente para asuntos relacionados con las actividades de la PROCONVET S.A.

ARTÍCULO 13. Instalación y mantenimiento de los equipos. El área de sistemas deberá llevar un inventario de todos los equipos propiedad de la PROCONVET S.A.

Los equipos que deban o estén conectados a la red de la PROCONVET S.A. deberán estar sujetos a los requerimientos de instalación emitidos por El área de sistemas y tener la configuración de seguridad básica exigida por ella.

Es deber del responsable del equipo en conjunto con El área de sistemas dar cumplimiento a los requerimientos de instalación e informar sobre cualquier cambio que afecte la instalación del equipo. El responsable del equipo debe velar por la integridad física del equipo.

Es responsabilidad de El área de sistemas del mantenimiento preventivo y correctivo de los equipos propiedad de la PROCONVET S.A. El área de sistemas puede otorgar mantenimiento preventivo y correctivo cuando lo estimen necesario, con previó aviso al responsable del equipo.

Se debe procurar mantener actualizados los equipos con el fin de mantener el buen funcionamiento de éste o mejorarlo.

Cuando se requiera reutilizar cualquier dispositivo se debe borrar la información que contenga mediante el uso de técnicas que permitan que dicha información no pueda ser recuperada.

En caso de que se necesite dar de baja un dispositivo, este debe ser destruido físicamente de tal forma que no pueda recuperarse la información.

Los equipos que vayan a ser reutilizados o eliminados deberán ser revisados, con el propósito de no eliminar software licenciado, ni información confidencial de los cuales no se tenga copia.

Se deberá contar con autorización previa de El área de sistemas para la reutilización o eliminación de un equipo.
Para cada equipo eliminado se deberá tener un documento que contenga el motivo por el cual se da de baja, el responsable en dar de baja el equipo, la fecha y cualquier otra información que se considere importante.

CAPÍTULO IV.
ACCESO REMOTO

ARTÍCULO 14. Acceso remoto desde un entorno de internet. Se deben implementar protocolos capaces de cifrar la comunicación que se establezca desde el exterior de la red en la cual se transmita información sensible.

El área de sistemas es la encargada de asignar los correspondientes accesos remotos a los servicios de la red con autorización del responsable del servicio, en los casos que la criticidad del servicio lo amerite, por ejemplo, acceso mediante VPN o sesión Telnet.

ARTÍCULO 15. Desarrollo de servicios de red. La implementación de los servicios de red deberá tener el visto bueno del área de sistemas.

Al responsable del servicio de red le corresponde la implementación de la protección adecuada.

La programación e implementación de los servicios de red deberán estar de acuerdo con los requerimientos emitidos por el área de Informática.

CAPÍTULO V
MANEJO DE LA INFORMACIÓN

ARTÍCULO 16. Backup de la Información. La información que para la PROCONVET S.A. se considere crítica o sensible deberá tener copias de seguridad.

ARTÍCULO 17. Manejo de la información. El usuario no deberá divulgar o revelar información confidencial de la PROCONVET S.A. a personas no autorizadas. En caso de ser necesario compartir información confidencial con cualquier persona, entidad o firma fuera de la PROCONVET S.A., se debe solicitar autorización al área de sistemas o el oficial de protección de datos, quienes a su vez darán el manejo adecuado para dicha solicitud.

Dentro de la PROCONVET S.A., la información confidencial se revelará a aquellas personas cuyas funciones ameriten tener tal conocimiento. Aquellas personas que manejan información confidencial no deberán revelarla a ninguna otra persona de la PROCONVET S.A. Ningún usuario tiene, automáticamente, derecho a acceso a toda la información de la organización.

La persona que recibe información confidencial no deberá reproducirla, a menos que se le autorice por parte del dueño de la información. En caso de que se autorice realizar copias de la información suministrada, éstas deben ser controladas.

ARTÍCULO 18. Evaluaciones de seguridad. Las evaluaciones de seguridad deberían realizarse con regularidad con el fin de identificar posibles vulnerabilidades en el sistema. Toda información necesaria para la evaluación que se le suministre al evaluador o evaluadores deberá ser entregada bajo un compromiso de confidencialidad, que garantice no sea divulgada. El proceso de evaluación debería ayudar a encontrar las vulnerabilidades del sistema y a su vez los controles de seguridad adecuados para minimizarlas.

El proceso de evaluación debería asegurar que los resultados se documenten y hacerlo con regularidad podría ayudar a mejorar la Política de Seguridad.

CAPÍTULO VI.
MEDIDAS DE SEGURIDAD INFORMÁTICA

ARTÍCULO 19. Hacer Uso de Protocolo de Buenas Contraseñas. Las contraseñas de la PROCONVET S.A.:

1. No debe tener menos de ocho dígitos.
2. Mezclar mayúsculas y minúsculas, letras, números y caracteres especiales.
3. No debe contener nombres obvios o referentes a la organización.
4. Debe cambiarse frecuentemente.

ARTÍCULO 20. Hacer Uso de Encriptación de Datos. La Compañía hará un cifrado de datos con lo que logrará que:

1. Nadie lea la información en el transcurso de su envió.
2. Garantizar que el remitente sea quien dice ser.
3. El contenido del mensaje no sea modificado en el camino.

ARTÍCULO 21. Hacer Uso de Software de Seguridad. La Compañía podrá hacer uso de los siguientes softwares de seguridad:

1. El antivirus: estos detectan e impiden que se ejecute y elimina el software malicioso.
2. El cortafuego: con ello permitimos o prohibimos la comunicación entre el software de nuestro equipo e Internet y evitar que atacantes haga funcionar una aplicación en nuestro ordenador sin autorización.
3. Software Antispam: estos son filtros que detectan el correo indeseado.
4. Software Antispyware: estos programas son orientados a la detección, bloqueo y eliminación de software espía.
5. Filtros anti-phishing
6. Programas de monitorización wifi
7. Hacer uso de defensas pasivas

ARTÍCULO 22. Partición de Disco Duro o Sistemas Raid. La compañía podrá hacer partición de sus discos duros para, de esta manera, guardar los datos en una partición distinta a la que se utiliza para instalar el S.O, en caso de tener que formatear el equipo no se necesita sacar todos los datos.

Otra forma es tener en nuestro sistema un RAID o arreglo de discos, de tal forma que si existen daños en el disco duro principal este con replica en un segundo y no se pierda la información.

ARTÍCULO 23. Implementar un Controlador de dominio. Con el fin de facilitar la administración de las cuentas de usuario, equipos en la red, carpetas compartidas, permisos y control de acceso, además de asegurar, en gran parte del cumplimiento de la política de seguridad, se recomienda la implementación de un servidor de dominio que permita agrupar los equipos y usuarios dentro de un dominio. De esta manera, cada persona que acceda a los recursos de la red se identifica con un único

usuario, lo que facilita la auditoría de usuarios, ya que se puede rastrear los sucesos de cada uno de éstos, permitiéndole al administrador saber que usuario es el que comente una violación a la seguridad.

También permite una mejor administración de las directivas de seguridad para todos los usuarios, porque no se requiere definir directivas en cada equipo conectado a la red.

ARTÍCULO 24. Filtrado por MAC de conexiones físicas en la intranet. Una medida para evitar conexiones a la red de equipos no aprobados es filtrar por MAC. Esto ayuda a los administradores a saber que equipos están conectados a la red, y estar seguros de que cumplan con los requerimientos exigidos para operar de forma segura, de esta forma se reduce en significativamente que usuarios conecten equipos infectados y se propague un virus a los demás equipos.

ARTÍCULO 25. Implementación de detección o prevención de intrusos (IDS o IPS). PROCONVET S.A. podrá implementar un sistema de detección de intrusos (IDS) el cual está diseñado para detectar cualquier acceso no autorizado, ataque informático o cualquier violación a un equipo o a una red.

Un sistema de prevención de intrusos (IPS) es un dispositivo capaz de realizar las funciones de un IDS más las de prevenir las violaciones informáticas detectadas en la red.

Como medida técnica para reducir los ataques informáticos, se recomienda la implementación de estos sistemas en la red, que le permita a los administradores detectar con mayor facilidad de donde proviene los ataques y poder prevenir el éxito de éstos.
Hay dispositivos como los UTM que integran estas funcionalidades aparte de tener un sistema de firewall, control de acceso, filtrado de aplicaciones, filtrado de sitios web, control de VPN entre otras características.

CAPÍTULO VII.
BUENAS PRÁCTICAS PARA PROTECCIÓN DE DATOS PERSONALES

ARTÍCULO 26. Buenas prácticas. Todo el personal que acceda a información de PROCONVET S.A. está obligado a conocer y observar las medidas, normas, protocolos, reglas, estándares y políticas que afecten a las funciones que desarrolla.

ARTÍCULO 27. Cada persona se responsabiliza del puesto de trabajo que tiene asignado y debe cumplir con los procedimientos internos de PROCONVET S.A. con respecto a la protección de datos personales así:

1. Deberán guardar la confidencialidad de la información que conozcan en el desarrollo de su trabajo. Esta obligación de guardar secreto subsistirá aún después de finalizar las relaciones contractuales con la organización.

2. Evitar revelar información corporativa, salvo en aquellos casos en que el desempeño de las funciones laborales así lo requieran. No sacar información ni datos personales de la organización salvo en los casos que lo requieran las funciones asignadas y, en su caso, con previa autorización.
3. Cuando se abandona el puesto de trabajo, bien temporalmente o bien al finalizar el turno, se debe dejar en un estado que impida la visualización de los datos protegidos: bloqueando el equipo con contraseña o desconectándose de las aplicaciones y la red, y apagando el monitor.

4. Frente a cualquier solicitud de ejercicio de derecho de acceso, rectificación, cancelación u oposición de los datos por parte de su titular, informar inmediatamente reenviando dicha solicitud a la dirección de correo establecida como canal de comunicación por la organización, teniendo claro que existen unos plazos legales ajustados para responder a dichas solicitudes.

ARTÍCULO 28. Con respecto a los computadores portátiles y demás de dispositivos de almacenamiento móviles (teléfonos móviles, memorias USB, etc.), se debe cumplir:

1. Mantenerlos siempre controlados, (no dejar en lugares públicos, taxis, etc.) para evitar su sustracción.

2. Reducir y/o eliminar la información que no vaya a ser utilizada.

3. En caso de pérdida o robo de un dispositivo de almacenamiento móvil (portátil, teléfono, memoria USB, etc.) se notificará inmediatamente como incidencia de seguridad al área de sistemas o encargada.

4. Se debe proporcionar la ayuda que se requiera en lo que se refiere a mantener la calidad de los datos, lo cual implica controlar:

   a. Que la información contenida en los ficheros únicamente sea tratada en relación con las finalidades para las que se haya obtenido.

   b. Que los datos sean exactos, estén actualizados y sean cancelados cuando éstos hayan dejado de ser necesarios.

ARTÍCULO 29. Respecto al uso del correo electrónico e Internet, se debe prestar atención al envío de datos de carácter personal por medio del correo electrónico, tanto en el cuerpo del mensaje como en anexos y, si se realiza, deberá tratar esos mensajes y anexos como temporales y borrarlos en cuanto dejen de ser necesarios.

ARTÍCULO 30. No se podrán utilizar cuentas de correo personales para el envío de información profesional de la organización, excepto en situaciones inevitables como por ejemplo cuando exista una urgencia y el sistema esté caído.

ARTÍCULO 31. Ficheros temporales creados extrayendo datos de las aplicaciones corporativas para la ejecución de una determinada tarea o proceso (ejemplo: listados en Word o Excel) no deben mantenerse indefinidamente ni en el ordenador ni en un directorio de red y una vez finalizada dicha tarea o proceso hay que eliminarlos.

ARTÍCULO 32. Mesas limpias: cada usuario, cada vez que se ausente de su mesa de trabajo o bien cuando termine su jornada laboral, deberá retirar toda aquella información que contenga información que pudiera ser de carácter confidencial.

ARTÍCULO 33. Utilización de fotocopiadoras, escáneres e impresoras: Al utilizar impresoras o fotocopiadoras, debe asegurarse de recoger los originales al finalizar y de que no quedan documentos con datos sensibles en la bandeja de salida. Si las impresoras son compartidas con otros usuarios sin acceso a los datos que están siendo impresos, se deberán retirar los documentos conforme vayan siendo impresos.

ARTÍCULO 34. El personal que intervenga en el tratamiento de la información y que incumpla lo descrito en el presente documento, normas o procedimientos relacionados con la seguridad y con la protección de datos de carácter personal, deberá saber que podrá ser sometido al régimen sancionador/disciplinario existente en la organización, así como a Ley 1581 de 20102 y del Código Penal respecto a la comisión de delitos informáticos. Todo ello sin perjuicio de las posibles consecuencias civiles y penales a las que hubiera lugar en su caso.

ARTÍCULO 35. Fecha de entrada en vigencia de la política de seguridad de la información. La Política de seguridad de la información de PROCONVET S.A. entró en vigencia a partir del 21 de 12 de 2023.

La presente política fue actualizada el 20 de 12 de 2023.

JOHNIER PAVAS
REPRESENTANTE LEGAL
PROCONVET S.A.

ELABORÓ	REVISÓ	APROBÓ
FIRMA: N. Murcia	FIRMA: A. Pavas	FIRMA: J. PAVAS
NOMBRE: Nancy Murcia P	NOMBRE: Alejandra Pavas O	NOMBRE: Johnier Pavas M
CARGO: Coord. Administrativa	CARGO: Coord. Talento Humano	CARGO : Gerente General
FECHA : 2023-12-21	FECHA : 2023-12-21	FECHA : 2023-12-21