POLITICA DE SEGURIDAD INFORMATICA

POLITICAS DE SEGURIDAD INFORMATICA

INTRODUCCION

Foncaldas en cumplimiento de las normas ISO 27001:2013 y el Anexo Numero II Título IV, Capítulo IV de la Circular Básica contable y Financiera expedida por la Superintendencia de la Economía Solidaria, establece las políticas que integran el Sistema de Gestión de Seguridad de la Información SGSI, las cuales deben ser adoptadas por los directivos, administrativos, empleados, contratistas, aliados estratégicos y terceros que presten sus servicios o tengan algún tipo de vínculo contractual con el Fondo.

OBJETO

Generar una adecuada seguridad y protección de la información de Foncaldas, a través de políticas y directrices impartidas por los directivos.

ALCANCE

Aplica para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, administrativos, empleados, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con FONCALDAS, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación tanto en las medidas preventivas como correctivas.

TERMINOS Y DEFINICIONES

La seguridad de la información se define aquí como la preservación de las siguientes características o atributos:

Activo	Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos de Foncaldas. Se pueden clasificar de la siguiente manera: - Datos: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en el Fondo. Ejemplo: archivo de Word, Excel, entre otros.

	- Aplicaciones: Es todo el software que se utiliza para la gestión de la información. Ejemplo: Software contable, plataforma de facturación electrónica, entre otros. - Personal: Es todo el personal de Foncaldas, el personal subcontratado, los clientes, asociados, e general, todos aquellos que tengan acceso de una manera u otra a los activos de información del Fondo. - Servicios: Son tanto los servicios internos, tales como el crédito, ahorro, entre otros como los externos, aquellos que el Fondo suministra a los clientes y usuarios. Ejemplo: servicio de alojamiento, pasadía entre otros. - Tecnología: Son todos los equipos utilizados para gestionar la información y las comunicaciones - Instalaciones: Son todos los lugares en los que se alojan los sistemas de información. Ejemplo: servidor
Confidencialidad	Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
Declaración de aplicabilidad	Documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de Foncaldas.
Disponibilidad	Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
Integridad	Propiedad de salvaguardar la exactitud y estado completo de los activos.
Seguridad de la información	Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además para involucrar otras propiedades tales como. Autenticidad, trazabilidad y fiabilidad.

Sistema de gestión de la seguridad de la información (SGSI)	Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

POLITICA DE SEGURIDAD DE LA INFORMACION.

Políticas Generales: Se establece como política las siguientes:

- Garantizar la integridad, confidencialidad y disponibilidad de la información del Fondo de Empleados Universidad de Caldas - FONCALDAS manteniendo prácticas seguras en todos los procesos, con el propósito de no ser utilizado por individuos u organizaciones que quieren cometer actos ilícitos, avalando la satisfacción e imagen de nuestros servicios.

- Establecer un programa que permita el fomento continuo de la creación de cultura y conciencia de los diferentes usuarios de los sistemas de información y telecomunicaciones Foncaldas.
- Todos los usuarios autorizados para administrar la información de Foncaldas tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en la presente política.

- Evaluar la eficacia de la política de seguridad de la información, mediante el desarrollo de las diferentes etapas (Identificación, medición, control y monitoreo).

- Foncaldas debe contar con dispositivos y sistemas de seguridad perimetral para la conexión a Internet o cuando sea inevitable para la conexión a otras redes en outsourcing o de terceros.

- Los líderes de Área deben asegurarse de que los procedimientos de seguridad de la información dentro de su área de responsabilidad se realicen correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información.

- La Gerencia en apoyo con la Junta Directiva, son los encargados y responsables de que se implementen los controles necesarios para resguardar los sistemas de información, ya que este es el activo más importante de Foncaldas.

- Para garantizar la seguridad confidencial y el manejo de la información, se deben generar campañas de concientización continua en temas como; manejo y

asignación de contraseñas seguras, manejo adecuado y seguro en todo tipo de acceso a plataformas locales o externas, últimas tendencias de ilícitos informáticos y demás temas en seguridad.

- Las empresas externas que ofrecen servicios complementarios (internet, hosting, certificados, hacking ético, soporte y desarrollo) deben firmar entre las partes acuerdos de confidencialidad y pólizas de cumplimiento que permitan generar responsabilidad en las labores que se realizan.

- Toda adición tanto de software como de hadware a los equipos de cómputo debe solicitarse mediante formato a la Gerencia, quien designará un empleado encargado.

- Definir el calendario de días no laborales en el integrador, con el propósito de llegar un control al acceso de este.

- Definir permisos de horario extendido para empleados que lo requieran, esto se debe definir y parametrizar en el integrador para un mayor control.

- En la plataforma web, se requiere instalar un certificado digital de Seguridad de sellos mundialmente reconocidos para garantizar que toda la información que se genere maneje altos niveles de encriptación.

    - Dado el ágil avance de las tecnologías utilizadas para los desarrollos, se debe realizar mínimo cada año, un Hacking Ético tanto a la plataforma web como a la red interna.

    - El uso de recursos o servicios informáticos de Foncaldas este sujeto a monitoreo por parte del área de sistemas.

    - La creación de usuarios, el acceso y privilegios deben ser autorizados por el administrador del sistema.

    - Por seguridad, se deben definir perfiles de usuario según el cargo, dando los mínimos permisos sobre cada recurso informático a los usuarios que permitan su normal operación.

    - Los usuarios de equipo informático en forma compartida o individual son responsables de este, de velar por su integridad, del uso que se le de a la cuenta de red, correo y acceso a Internet. Al igual que los datos son de su exclusiva responsabilidad.

    - Los contratistas, proveedores y terceros que tengan acceso a los activos de

la información, están obligados a cumplir las políticas de seguridad de la información que la entidad establezca para mayor tranquilidad de los procesos.

- Se debe dar de baja a todos los equipos que no se vayan a utilizar en el Fondo, eliminando toda la información vulnerable que contenga, incluido licencias).

- Se deben desactivar todos los usuarios de empleados que sean desvinculados de Foncaldas

Manejo de información

No se permite el uso de los bienes y servicios informáticos para:

- Distribuir, entregar o divulgar a terceros información confidencial reservada o estratégica de Foncaldas, salvo autorización previa y expresa y que tenga que ver con el cumplimiento de las funciones de cada empleado, para ello debe haber firmado previamente el acuerdo de confidencialidad establecido por Foncaldas.

- Usar, alterar o acceder sin autorización los datos de otros usuarios.

- Suplantar a otras personas, haciendo uso de las claves de acceso ajenas a los servicios.

- Interceptar o alterar la información que se transmite.

- Sacar o tomar prestados los recursos informáticos sin la debida autorización.

- Interferir deliberadamente el sistema o el trabajo de otros, por ejemplo, ejecutando códigos dañinos tales como virus.

- Realizar tareas no relacionadas con actividades propias de Foncaldas.

- Utilizar la infraestructura de tecnología de información de Foncaldas para conseguir o transmitir material con ánimo de lucro.

- Hacer ofrecimientos fraudulentos de productos o servicios cuyo origen sean los recursos o servicios propios de Foncaldas.

- Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios.

- Hacer copia no autorizada de material propio del Fondo o de material protegido por derechos de autor.

- Violar estas u otras políticas o reglamentos internos de Foncaldas.

- Permitir o facilitar que usuarios no autorizados hagan uso de los recursos tecnológicos de Foncaldas.

- Utilizar los equipos de cómputo o dispositivos móviles para almacenar archivos, música, fotos, videos, juegos o similares que no tengan relación con Foncaldas.

- No se debe utilizar las unidades de red para manejo de información personal.

- Llevar a cabo actividades fuera de la ley.

Manejo de dispositivos

No se permite:

- Utilizar memoria USB no perteneciente a Foncaldas, CD, cámaras, celulares o cualquier otro dispositivo cuyo contenido sea desconocido en el equipo, sólo debe tener acceso a estas unidades externas el administrador del sistema, debido a la vulnerabilidad ante los virus, robo de base de datos, ingreso de virus troyanos, posibles fraudes entre otros.

- Utilizar usb, cd-rom u otros dispositivos prestados por alguien para instalar programas o abrir archivos, ya que este proceso es inseguro e igualmente solo lo debe hacer la persona encargada de sistemas.

Antivirus

Los virus pueden causar daño sustancial al sistema de cómputo, cada usuario tiene la responsabilidad de tomar las precauciones necesarias. Para evitar ingreso y propagación de virus, troyanos, spam, spyware se debe tener en cuenta lo siguiente:

- Todos los equipos pertenecientes a Foncaldas deben tener un antivirus efectivo y actualizado.

- Los equipos con acceso a Internet deberán actualizar y ejecutar el antivirus diariamente.

- Todos los equipos de Foncaldas deberán ser examinados en su totalidad, una vez a la semana, por el antivirus.

- Cualquier archivo de origen ajeno al equipo, debe ser revisado por el antivirus, sin importar el medio de almacenamiento de éste (CD, usb o compartido en red).

- Revisar el contenido de archivos comprimidos y correos electrónicos.

- Si durante el proceso de revisión de algún medio de almacenamiento se detecta algún virus, el archivo debe ser inmediatamente eliminado.

- Los equipos que no son de propiedad de Foncaldas pero que de igual manera se conecten a la red deben ejecutar un software de antivirus actualizado.

- No compartir carpetas, solo cuando sea absolutamente necesario y con las personas que lo necesiten, dándole seguridad a los datos.

Copias

- Se deben realizar copias de seguridad de los sistemas del software contable diariamente y de forma completa cada 7 días almacenados en medio externo (NAS), también se debe tener otra copia que será almacenada en un lugar externo a la sede (Backup en la nube).

- Se debe realizar copias de seguridad del sistema de información Sicses en equipo local, guardando una copia mensualmente en disco externo.

- Realizar copias de los correos oficiales entrantes o salientes de la entidad en forma mensual. Medio externo.

- Backup de Páginas Web, Información: Todo el directorio raíz que contiene la estructura, base de datos, contenido y multimedia cada vez que se incremente considerablemente la información

Contraseñas

- Todas las contraseñas son de carácter confidencial, intransferibles y de uso individual.

- No compartir las contraseñas de acceso con otros usuarios de los sistemas.

- No revelar las contraseñas ó código de su cuenta por ningún medio de comunicación ó directamente a otros (por ejemplo, su cuenta de correo electrónico, su usuario de bases de datos o permitir su uso a terceros para actividades ajenas a la misión de Foncaldas. La prohibición incluye familiares y cualquier otra persona que habite en la residencia del funcionario cuando la actividad se realiza desde el hogar o un punto de atención, (por ejemplo, computadores portátiles, teléfonos celulares, tabletas).

- Cuando se tenga que entregar equipos de cómputo o dispositivos móviles a otros funcionarios o encargados, se debe hacer mediante acta de entrega solicitando nuevas contraseñas y códigos de seguridad cuando aplique.

- Las contraseñas de acceso a los equipos de cómputo como al sistema de información financiero deben ser renovadas cada 60 días.

- Se deben establecer contraseñas seguras y personalizadas para los usuarios que accedan remotamente a la red del Fondo, generando responsabilidades sobre estos funcionarios en el manejo de dichos accesos.

- No utilizar las funciones “recordar contraseña” que poseen algunas aplicaciones.

- No escribir las contraseñas en ningún documento que se encuentre en su lugar de trabajo.

- Se debe evitar utilizar la misma contraseña siempre en todos los sistemas o servicios

Guía de Generación de Contraseñas:

Para la definición de contraseñas a usar por parte de los usuarios se deben considerar las siguientes características:

- Caracteres en mayúsculas y minúsculas (por ejemplo a -z, A-Z)

- Contener caracteres especiales (por ejemplo */-_+)

- Las claves de los usuarios con privilegios (0 de servidores) deben cambiarse mínimo cada mes y las claves de losusuarios sin privilegios deben cambiarse mínimo cada dos meses.

- No debe estar basada en información personal, nombres de familia, número de cédula, fecha de nacimiento etc.

- Las contraseñas no deben ser nunca almacenadas en un equipo de cómputo.

- Se debe tratar de crear contraseñas que puedan ser recordadas fácilmente y que pueda escribirse rápidamente.

- Para la seguridad de los equipos en el puesto de trabajo se configurará el salvapantallas para cuando se presente una inactividad de más de 10 minutos se bloquee y pida contraseña para su ingreso.

Correo electrónico e internet

- Los mensajes enviados a listas de correo o grupos de discusión por los integrantes de Foncaldas y que utilicen las direcciones de correo de las entidades deben contener un párrafo donde diga “AVISO LEGAL”.

El contenido de este correo electrónico, sus archivos adjuntos y enlaces, es confidencial y privilegiado, por lo que sólo podrá ser utilizado por la entidad o persona a la cual está siendo dirigido y únicamente para las finalidades indicadas en el mismo. En caso de que usted no sea el destinatario real, y por error haya recibido el presente correo, lo invitamos a que notifique el hecho por este medio y proceda a eliminarlo inmediatamente, absteniéndose de modificar, circular, difundir, reproducir o divulgar de cualquier forma o por cualquier medio, su contenido total o parcial.

Los datos personales que se recolectan por este medio, serán tratados por FONCALDAS, NIT 890.801.733-7, en calidad de Responsable del Tratamiento de Datos Personales, conforme a lo dispuesto por nuestra Política de Privacidad y Protección de Datos Personales, la cual puede ser consultada en la página web www.foncaldas.com. Como Titular de Datos Personales, usted tiene el derecho de conocer, actualizar y rectificar la información personal que repose en nuestras bases de datos. Para mayor información, puede comunicarse con nosotros a través del correo electrónico contacto@foncaldas.com, o directamente en las instalaciones del responsable del Tratamiento ubicadas en Manizales en la Calle 60 No. 25 – 01 barrio estrella.

- Nunca se debe abrir un adjunto de un email sin antes chequearlo con el antivirus. Si el adjunto es de un desconocido que no da avisópreviamente del envío del material, directamente borrarlo sin abrir.

- Está prohibido enviar mensajes de correo no solicitados, incluyendo junk mail (material publicitario enviado por correo) o cualquier otro tipo de anuncio comercial desde el correo interno (email spam, mensajes electrónicos masivos, no solicitados y no autorizados en el correo electrónico).

- Está prohibido generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.

- Está prohibido el envío de mensajes de correo electrónico con una dirección de correo diferente al verdadero remitente con el fin de realizar algún tipo de acoso, difamación u obtener información.

- No está permitido utilizar las cuentas de correo corporativas para recibir o enviar correo personal.

- No se debe utilizar el correo electrónico personal para enviar ó recibir información de Foncaldas.

- Por razones de seguridad y riesgos asociados se prohíbe el ingreso a páginas no autorizadas por el Fondo. Solo se autorizarán las páginas estrictamente necesarias para el desarrollo de las funciones del cargo.

- Foncaldas puede utilizar software para identificar y bloquear sitios de internet con material inadecuado, violento y sexuales explicito. En el evento, que el usuario encuentre este tipo de material en internet, deberá desconectarse del sitio en forma inmediata, sin importar si el sitio ha sido bloqueado o no por el software.

- Se prohíbe el uso de software de mensajería instantánea como Messenger, Facebook, twitter chats o similares que determinan la salida de información confidencial de la entidad a menos que se justifique el uso de este, este debe ser solicitado y debe ser autorizado por un administrador del Fondo.

- No utilizar el Internet para descargas de programas o trabajos de dudosa procedencia.

- No se podrá acceder remota o directamente a un equipo sin el debido permiso; cuando se requiera acceder remotamente a un equipo de la empresa, se deberá

utilizar únicamente conexiones seguras como VPN, ANYDESK o TEAMVIEWER.

Software:

- Se prohíbe exportar software, información técnica, entregar la base de datos sin autorización.

- Está prohibido explícitamente el monitoreo de puertos o análisis de tráfico de red con el propósito de evaluar vulnerabilidades de seguridad. Las personas responsables de la seguridad informática pueden realizar estas actividades cuando se realicen en coordinación con el personal responsable de los servidores, los servicios, las aplicaciones y de la red.

- El uso de Software libre está permitido siempre y cuando el funcionario lo solicite a la Gerencia, explicando el uso y la descripción del software a instalar.

- El Software instalado debe ser actualizado cada vez que haya una actualización disponible si se considera necesario.

- Las actualizaciones Automáticas de los sistemas operativos deberán estar elegidas con la opción de notificación previa para descarga, a partir de esto seleccionar los paquetes de actualización relacionados con parches de seguridad y otras necesarias.

Protección de Información y Hadware

- El área encargada debe mantener bajo su resguardo el software que se utiliza en Foncaldas, los medios de instalación CDs originales, licencias, manuales y garantías de equipos.

- Se deben establecer los controles necesarios para mantener la información protegida. (Firewall, antivirus, monitoreo de puertos, protocolos, copias de respaldo, mantenimiento de equipos, software, red, criptografía (La criptografía consiste en cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que sólo puedan ser leídos por las personas a quienes van dirigidos). Se recomienda el uso de criptografía para la información que los usuarios consideren sensitiva o vulnerable.

- Se debe informar a los grupos de interés sobre la salida de personal clave del Fondo.

- Para prevenir la pérdida de datos por corte abrupto de la energía eléctrica, los usuarios deben grabar periódicamente sus archivos de datos cuando se encuentren trabajando en cualquier herramienta o software de propósito específico.

- No se debe compartir los tomas de su equipo (COLOR NARANJA) con otros aparatos de diferente especificación como celulares, lámparas, secadores de cabello, brilladoras, taladros, impresoras, sumadoras. Estos pueden provocar cambios transitorios bruscos de voltaje, que pueden llegar a dañar el equipo o producir pérdida de información.

- El equipo se debe conectar únicamente a tomacorrientes que pertenezcan al circuito eléctrico exclusivo para ellos, con protección contra sobrevoltajes transitorios (cortapicos) o ups.

- Cuando se presenten tempestades, los equipos se deben desconectar, pues las descargas eléctricas pueden ocasionar daños, especialmente si están conectados a una línea telefónica a través de módem.

- En caso de tener que mover los equipos por cualquier razón verificar que estén apagados, evitar movimientos bruscos o traslados frecuentes que puedan ocasionar problemas; en consecuencia, para evitar que se dañen.

- Los dispositivos móviles e impresoras térmicas no se deben dejar cargando toda la noche.

- Se debe almacenar, solo los archivos de datos que sean estrictamente necesarios y borrar o descargar aquellos que no se requieran de acuerdo con la necesidad y la importancia de cada uno de ellos.

- Los dispositivos (token) utilizados para ingreso a páginas de bancos deben estar en sitios seguros.

- Las chequeras, Cdts y sellos deben estar en sitios seguros fuera del alcance de personas no autorizadas.

Política de seguridad para los recursos humanos

- Foncaldas implementa acciones para asegurar que los empleados y demás colaboradores del Fondo, asuman sus responsabilidades, como usuarios y roles asignados, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información.

- Los empleados y demás colaboradores del Fondo deben dar aprobación para el tratamiento de sus datos personales de acuerdo con la Ley 1581 de 2012, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.

- El empleado o colaboradores del Fondo, previo a la posesión del cargo, deberá diligenciar el formato de conocimiento del cliente.

- Se debe capacitar y sensibilizar a los funcionarios durante la inducción sobre las políticas de seguridad de la información, ciber seguridad entre otros.

Vacaciones Empleados

- Programar vacaciones del personal que maneje dinero como cajeros, tesoreros, quienes manejan recaudo empresarial, recaudo externo, débitos automáticos, conciliación bancaria y los procesos que el Fondo considere críticos una semana antes del corte del mes y se les den los 15 días hábiles completos y asignarles estas tareas a personal que pueda realizar y auditar el trabajo del empleado que salió a disfrutar las vacaciones.

- Desactivar los usuarios de los equipos de cómputo, correo electrónico, sistemas de conexión remota y aplicaciones de trabajo toda vez que un empleado salga a disfrutar de su periodo de vacaciones.

Comité de seguridad interdisciplinario

La Gerencia, debe apoyar activamente la seguridad de la información dentro del Fondo con un objetivo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades frente a la seguridad de la información. Este compromiso se verá reflejado a través de:

- Creación de un comité de seguridad interdisciplinario incluyendo el Área TI (Tecnología de Información).

- Asignación de un responsable de la seguridad de la información (Oficial de Seguridad).

- Aprobación del documento de políticas de seguridad de la información.

- Velar por el cumplimiento de las políticas de seguridad de la información.

- Asignación de responsabilidades asociadas al tema de la seguridad de la información.

- Definición y aprobación de los planes de continuidad y contingencia
- Políticas de backups
- Proveer los recursos necesarios para minimizar los riesgos tecnológicos.
- Elaborar y conocer la matriz de riesgos, esto permitirá implementar acciones para mitigar los riesgos de seguridad de la información.

VIGENCIA.

La presente política rige a partir de su aprobación por parte de la Junta Directiva derogando toda norma anterior y como constancia de su aprobación está el Acta Número _____ del ____ de _____ de 2024.

Gestión del Cambio:

Fecha	Versión	Descripción De Cambios

MARIA DEL SOCORRO CANDAMIL CALLE
Presidenta Junta Directiva

JOSE ARTEMO ACEVEDO LOPEZ
secretaria Junta Directiva