VISIONAMOS
sistema de pago cooperativo

POLÍTICAS ESPECIFICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

TABLA DE CONTENIDO.

1. INTRODUCCIÓN.

VISIONAMOS SISTEMA DE PAGO COOPERATIVO establece su compromiso con el Sistema de Gestión de Seguridad de la Información y Ciberseguridad definiendo la política S-SI-R-04-Política Sistema de Gestión Integrado, adicional a ella establece el presente documento en el que se reúnen las diversas políticas específicas de seguridad de la información de la Entidad, con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información, entendidas como:

- ✓ Confidencialidad: Seguridad de que la información es accesible solamente a quienes están autorizados para ello.
- ✓ Integridad: Protección de la exactitud y estado completo de la información y métodos de procesamiento; y
- ✓ Disponibilidad: Seguridad de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

2. OBJETIVO.

Definir los lineamientos y las reglas básicas para la gestión de la seguridad de la información y ciberseguridad con el fin de efectuar una implementación transversal de los controles en la entidad.

3. ALCANCE.

Estas políticas deben ser acatadas por todos los colaboradores y personal externo que participe en la ejecución de los procesos de la Entidad.

4. POLITICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

4.1. POLÍTICA DE DISPOSITIVOS MÓVILES.

El uso de los dispositivos móviles se limita a los computadores portátiles que se utilizan para manejar la información. Para dar cumplimiento a esta política deben apoyarse en lo definido dentro de los siguientes procedimientos:

- ✓ PSGSI-01 Gestionar Monitoreo de Seguridad
- ✓ PSGSI-06 Gestionar Activos de Información

4.1.1. LINEAMIENTOS.

- ✓ El uso de cualquier equipo de almacenamiento y procesamiento de información por fuera de las instalaciones de la Entidad es aprobado por el jefe inmediato en caso de que el colaborador no esté dentro de la modalidad de Teletrabajo. Esto aplica a equipos de propiedad de la Entidad y a equipos de propiedad privada y usados a nombre de la entidad.

- ✓ Se debe contar con un inventario de activos actualizado de todos los portátiles que son suministrados por VISIONAMOS para la realización de las funciones correspondientes a su área y que se utilizan para procesar y/o transmitir información.

- ✓ VISIONAMOS establece lineamientos tanto para el acceso a sus redes inalámbricas, instalación de software y correo electrónico mediante el uso de los dispositivos, y asigna responsabilidades sobre los funcionarios, contratistas o terceros en la manipulación de la información manejada en dichos dispositivos.

- ✓ Los controles para lugares fuera de las instalaciones, tales como teletrabajo y sitios temporales se deben determinar mediante una valoración de riesgos y se deben aplicar los controles adecuados según sean apropiados. Por ejemplo, gabinetes de archivo con llave, política de escritorio limpio (S-SI-M-03-Sistema de gestión de seguridad de la información y Ciberseguridad, numeral 10.2.7 y dentro del manual S-SI-M-01-Uso aceptable de activos dentro del numeral 15), controles de acceso para computadores y comunicación segura con la oficina.

- ✓ En el caso de pérdida de un dispositivo de VISIONAMOS ya sea por hurto o cualquier motivo, se debe informar inmediatamente al Líder Administrativo, Jefe directo, y al Oficial y/o Analista de Seguridad de la Información con el fin de aplicar el procedimiento PSGSI-06 Gestionar Activos de Información que se tenga establecido en la Entidad.

- ✓ Es responsabilidad del usuario el uso correcto del dispositivo suministrado por VISIONAMOS con el fin de realizar las actividades y funciones correspondientes a su cargo. No se podrá utilizar el dispositivo con fines personales o en lugares donde exista algún riesgo de pérdida o robo.

- ✓ Todos los dispositivos suministrados por VISIONAMOS deben tener mecanismos de autenticación con el fin de permitir el acceso a la información del mismo.

- ✓ Se deben verificar todos los elementos de los equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reuso.

- ✓ Se deben generar tips de recomendación para el correcto uso del dispositivo y su cuidado físico. Cada uno de los funcionarios debe proporcionar un correcto uso al dispositivo fuera de VISIONAMOS.

- ✓ Los equipos y medios retirados de las instalaciones no se deben dejar sin vigilancia en lugares públicos.

- ✓ En VISIONAMOS aprueba el uso de los dispositivos móviles autorizados parte de los colaboradores de la entidad siempre y cuando no pongan en riesgo la Seguridad de la Información. Para ver más detalle ver el manual S-SI-M-03-Sistema de gestión de seguridad de la información y Ciberseguridad, numeral 5,2

- ✓ Los equipos portátiles pueden estar asegurados con la guaya o el mecanismo que se defina para su protección dentro o fuera de las instalaciones de la Entidad (Para mas detalle ver el manual S-SI-M-01-Uso aceptable de activos, numeral 9)

- ✓ Todas las estaciones de trabajo deben tener instalados el software antivirus.

- ✓ Todas las estaciones de trabajo en la Entidad deben estar conectadas en el circuito protegido por la UPS.

- ✓ Para la administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de la Entidad, solo pueden realizar dicha actividad las personas que estén autorizada y se debe dejar registro de la autorización por cualquier medio de comunicación escrito. Las conexiones deben cumplir con los esquemas de seguridad definidos. (Ver S-SI-M-01-Uso aceptable de activos)

4.2.POLÍTICA DE TELETRABAJO.

VISIONAMOS, debe proteger la información a la que tienen todos los colaboradores que laboran en teletrabajo. Todo acceso y manipulación de la información es responsabilidad expresa de los colaboradores siguiendo lo establecidos por VISIONAMOS.

- ✓ Se debe usar la solución VPN o red virtual protegida (Virtual Protected Network) para acceder a redes corporativas.
- ✓ Se debe utilizar el doble factor de autenticación en todos los sistemas y tecnologías que lo permitan.

4.2.1. LINEAMIENTOS.

El teletrabajador se compromete a cumplir los requerimientos establecidos frente a la protección de datos (S-SI-R-01-Política Tratamiento de Datos Personales /S-SI-M-02-Manual Protección de Datos Personales), las políticas definidas en el manual T-AP-M-02-Manual de teletrabajo en el numeral 7.5; como también el cumplimiento de lo siguiente:

- ✓ Todo funcionario debe acoger las recomendaciones frente a los posibles riesgos tecnológicos para realizar las funciones desde su lugar de residencia.
- ✓ Toda conexión se debe realizar desde un dispositivo que sea propiedad de la entidad.
- ✓ Los funcionarios deben cumplir con los esquemas de trabajo que se han definido.
- ✓ No se permite el uso de dispositivos externos de almacenamiento (USB y discos externos).
- ✓ Los funcionarios en teletrabajo deben cumplir con las medidas de seguridad que VISIONAMOS haya implementado para asegurar la confidencialidad e integridad de los datos a los que tenga acceso.
- ✓ En caso de hurto o pérdida del equipo portátil utilizado para teletrabajar que contenga información de VISIONAMOS, se debe informar inmediatamente al Líder Administrativo, Jefe directo, y al Oficial y/o Analista de Seguridad de la Información con el fin de aplicar el procedimiento PSGSI-06 Gestionar Activos de Información que se tenga establecido en la Entidad, así mismo debe generar el denuncio ante las autoridades.
- ✓ Los equipos asignados a cada colaborador son responsabilidad de este y debe velar por su correcta custodia y forma de uso.

NOTA: La información aquí relacionada en el presente manual es complementada por los lineamientos definidos en el S-AP-R-06-Reglamento interno de trabajo / T-AP-R-06-Reglamento Interno de Trabajo.

4.3.POLÍTICA DE CONTROL DE ACCESO.

4.3.1. LINEAMIENTOS GENERALES.

- ✓ Solo los usuarios autorizados deben acceder a la información.
- ✓ Los accesos son creados bajo la regla del menor privilegio posible con el fin de minimizar las posibles afectaciones sobre la información.
- ✓ Para el ingreso a los sistemas de información se hace uso de usuario y contraseña, quiénes estén autorizados son responsables de las operaciones que se realicen haciendo uso de dichas credenciales y de su correcta custodia.
- ✓ Las credenciales proporcionadas por VISIONAMOS para el desarrollo de sus labores o prestación de un servicio son personales e intransferibles. Cada usuario es responsable de sus acciones.
- ✓ VISIONAMOS contempla la premisa del menor privilegio posible. Las cuentas de usuario tendrán asignados permisos específicos para acceder y realizar única y exclusivamente las operaciones autorizadas.
- ✓ La vigencia de la contraseña será de máximo sesenta (60) días y no se podrá utilizar la misma contraseña durante los siguientes diez (10) cambios de contraseña.
- ✓ Se tendrá habilitado en TODOS los sistemas que lo permitan, el múltiple factor de autenticación.
- ✓ La complejidad de las contraseñas será de mínimo ocho caracteres alfanuméricos, mayúsculas y caracteres especiales.
- ✓ Teniendo en cuenta que los proveedores, en pro de desarrollar sus funciones, deben contar con un acceso autorizado único por cada individuo, que será controlado por el dueño del activo, quien realizará revisiones periódicas de la utilización de los accesos y cualquier anomalía se tomará como un incidente y se aplicará el debido proceso. Para esto VISIONAMOS les asignará este acceso a través de un mecanismo de infraestructura tecnológica de VISIONAMOS que deje precedente las responsabilidades y buenas prácticas

de uso que este acceso implica. Además, se usará el mismo mecanismo para la devolución o revocación de este acceso cuando este aplique.

- ✓ Establecer una política de control de accesos que garantice solo a las personas autorizadas el ingreso a las diferentes áreas de la compañía con base a los requisitos del negocio y la seguridad de la información.

- ✓ En el momento de presentarse una solicitud para obtener acceso a algún recurso de VISIONAMOS se debe hacer el correspondiente análisis de riesgo teniendo en cuenta la clasificación de la información, con el fin de otorgar los privilegios de acceso correspondiente

- ✓ La asignación de los diferentes usuarios debe ser revisados cada seis (6) meses con el fin de validar algún cambio de perfil en los usuarios o reasignarse si es del caso.

- ✓ Se deben retirar inmediatamente los accesos a los colaboradores que hayan terminado su relación laboral con VISIONAMOS.

  NOTA: En caso de que el colaborar que se retira, atienda casos de la mesa de servicio, el Analista de Contratación y/o el Jefe Inmediato debe solicitar por un caso en la mesa de servicio al proceso de Gestión de Infraestructura y Telecomunicaciones el trasladen dichos casos a otro colaborar para su gestión para luego el proceso de Gestión de Seguridad de la Información procesa con el retiro de los accesos de dicho colaborador.

- ✓ Los privilegios de administración de cualquier máquina, desktops, servidor, etc, deben ser asignados solo al personal encargado de administrar los sistemas asociados al proceso de Gestión de Infraestructura y Telecomunicaciones y/o Gestión de Seguridad de la Información VISIONAMOS. Por ningún motivo se le deben otorgar estos privilegios a los usuarios de los equipos.

- ✓ Las contraseñas predeterminadas por el fabricante se deben cambiar inmediatamente después de la instalación de los sistemas o del software.

4.3.2. LINEAMIENTOS PARA LA REVOCACION DE CREDENCIALES Y MODIFICACIÓN DE LOS PERMISOS ASIGNADOS.

- ✓ Al finalizar la relación contractual con un colaborador, proveedor o cliente, VISIONAMOS debe inactivar de forma inmediata las credenciales asignadas.

- ✓ En caso de que alguno de los colaboradores sufra un cambio en sus funciones asignadas el Analista de Contratación debe generar un caso por la mesa de ayuda al Analista de Infraestructura con la debida autorización del proceso de Gestión de Seguridad de la Información, en donde solicite la modificación de su rol respectivo a los permisos asignados.

4.4. POLÍTICA DE CRIPTOGRAFÍA O CIFRADO DE LA INFORMACIÓN.

Dentro del manual S-SI-M-03-Sistema de gestión de seguridad de la información y Ciberseguridad en el numeral 9.1 se define criterios de criptografía. Así mismo en este documento se definen parámetros que se deben tener en cuenta para el correcto uso de controles criptográficos en la operación y los procesos de VISIONAMOS.

4.4.1. CONTROLES CRIPTOGRÁFICOS ESTABLECIDOS.

- ✓ La información que contenga contraseñas debe ser cifrada para su protección; no debe ser almacenada en texto plano.

- ✓ El acceso a los sistemas de información siempre se realizará por medio de protocolos seguros SSH, HTTPS.

- ✓ La comunicación e intercambio de información entre VISIONAMOS y sus clientes, colaboradores y proveedores siempre se realizará a través de canales seguros cómo son por ejemplo conexiones Correo Corporativo, SFTP, VPN Sitio a Sitio, VPN Cliente a Sitio.

- ✓ Se implementarán para el cifrado de información algoritmos de cifrado robustos, mínimo SHA256 y AES 256. VISIONAMOS se acoge a la política de cifrado de sus clientes teniendo como mínimo aceptable los algoritmos antes mencionados.

- ✓ Para las redes inalámbricas en las instalaciones de VISIONAMOS se implementará como mínimo WPA2/PSK AES.

4.4.2.LINEAMIENTOS PARA LA GESTIÓN DE LLAVES.

4.4.2.1. ESCENARIO DE CIFRADO.

✓ CIFRADO EN TRÁNSITO: La Plataforma de la entidad cuenta con certificados de seguridad SSL instalados en nuestros servidores para todos los ambientes - Desarrollo, Laboratorio y Producción. Esto garantiza que la información no puede ser interceptada para su eventual alteración o modificación durante su tránsito.

✓ CIFRADO EN REPOSO: La información crítica proporcionada por nuestros clientes es cifrada en las cuentas de almacenamiento, utilizando el algoritmo AES-256 proporcionado por nuestro Proveedor Cloud. Dicha información sólo es legible en el momento de su procesamiento.

4.4.2.2. ESCENARIO DE CIFRADO APLICACIONES WEB.

Para los servicios en cloud y aplicaciones que lo soporten las llaves de cifrado serán administradas por servicios de KMS - Key Management Service - para garantizar el cifrado de la información en reposo. (Ver el procedimiento Gestionar Llaves de Cifrado PSGSI-07)

✓ **INTERCAMBIO DE INFORMACIÓN CON CLIENTES:** Con las Entidades se debe realizar la creación de tres (3) llaves: Llave de compensación, llave de transferencia y llave enrutamiento. Las llaves no se guardan en VISIONAMOS quedan en la entidad, pero se deja registro en un repositorio.

Para el intercambio de información de estas llaves se le debe aplicar el Criptoperiodo dos (2) años.

✓ **INTERCAMBIO DE INFORMACIÓN CON DISPOSITIVOS:**

- Con los dispositivos es se generan las llaves y se matriculan en los Datafono y Pin Pad, estas llaves quedan grabadas (Solo Pin Pad) en los dispositivos, y se deja evidencia en el repositorio: Pin PAD
W:\VISIONAMOS SPBV\CONTROL Y MEJORA\SGI\3.SI Y CIBERSEGURIDAD\GESTIÓN DE LLAVES DE CIFRADO\FMSI-0804 Acta Generación Ingreso de Llaves\2022
- No tiene cambios ni vigencia.

✓ **INTERCAMBIO DE INFORMACIÓN CON SFTP CLIENTES:**

- Se generan las llaves XML (Infraestructura) de los sitios SFTP, se las envían al cliente y se deja registro de las llaves en la ruta:W:\VISIONAMOS SPBV\CONTROL Y MEJORA\SGI\3.SI Y CIBERSEGURIDAD\GESTIÓN DE ACCESOS\2021\PENDIENTE POR REVISION\CustodiaLlavesSFTP

4.5. POLÍTICA DE CONTROL DE ACCESO FISICO.

En VISIONAMOS el acceso a las instalaciones se realiza por medio de un sistema de control de acceso, para controlar la seguridad de los accesos, administrar los horarios, y controlar fácilmente las actividades que se realizan. Este sistema ha sido instalado en la entrada principal de la Entidad y en las puertas de acceso al Centro de Cómputo y de Comunicaciones.

✓ El Jefe inmediato en conjunto con Gestión de Seguridad de la información y/o Gestión Administrativa, analizan y autorizan el personal que puede tener acceso a las áreas restringidas, de acuerdo con las responsabilidades asignadas al cargo que desempeñan.

✓ El Sistema permite llevar un registro de quién realizó la apertura de una puerta y en qué tiempo. Sin la tarjeta y/o huella que contiene el código de identificación, las puertas que tienen los dispositivos instalados para su apertura permanecerán bloqueadas.

✓ El sistema implementado en VISIONAMOS, permite definir lo siguiente:

- Agenda (días y horarios)
- Perfiles (responsabilidades y área a la que pertenece el empleado
- Puertas (ingreso a la Entidad, ingreso al centro de cómputo y de comunicaciones).

✓ Los colaboradores pueden utilizar el sistema de control de acceso varias veces al día al ingresar a las instalaciones, quedando registrada en el sistema el primer ingreso, por lo que es fácil de usar y no requiere de una formación especial.

NOTA: Es de anotar que la seguridad de la organización no sólo es a través de los sistemas, también los colaboradores con las buenas prácticas, conductas y actuaciones son participes y generadores de la seguridad de la Entidad.

4.5.1. RIESGOS Y PRECUACIONES CON EL SISTEMA DE CONTROL DE ACCESO Y EL USO.

4.5.1.1. ACCESO Y USO.

El sistema de control de acceso en oportunidades puede presentar desincronizaciones y las mismas se pueden traducir en riesgos y peligros para la Entidad, en estos casos debemos ser diligentes y cuidadosos, cuando:

- ✓ Si varios empleados entran simultáneamente, el sistema podría dejar la puerta abierta. En estos casos, se debe constatar si la puerta quedo realmente cerrada.

- ✓ La tarjeta para el ingreso al Centro de Cómputo y de Comunicaciones, tiene el reverso el mensaje que es personal e intransferible, en caso de que a un colaborar se le extravié lo debe reportar por cualquier medio de comunicación al jefe inmediato y/o Analista de contratación quien se encargara de gestionarlo.

- ✓ El uso indebido de la tarjeta de ingreso al Centro de Cómputo y Comunicaciones dará lugar a sanciones legales o las contempladas en los reglamentos de la Entidad. El colaborador será el responsable de informar a la Entidad a fin de que esta sea bloqueada y se evite posibles accesos de terceros con la tarjeta extraviada.

- ✓ Los ingresos nocturnos a las instalaciones de la Entidad deben estar debidamente autorizados por el Líder Administrativo quien realizara la gestión para el ingreso. Para los efectos, solo están autorizados los Operadores del Sistema para ingresar de acuerdo con los horarios y turnos establecidos por la Entidad. El resto de los colaboradores no tiene autorizado el acceso en horario nocturno.

4.5.1.2. MECANISMOS DE CONTROL ÁREAS RESTRIGIDAS.

VISIONAMOS ha definido los controles de acceso a las áreas restringidas, mediante el manejo adecuado de los bienes e información de la Entidad, además de la seguridad de sus colaboradores:

- ✓ VISIONAMOS cuenta con un sistema biométrico en su puerta principal, el cual permite a los colaboradores la entrada controlada a las instalaciones.

- ✓ La habilitación de los colaboradores en el sistema biométrico para el ingreso a las instalaciones de VISIONAMOS estará a cargo del Auxiliar de Gestión de Personas.

- ✓ Los horarios de acceso a las instalaciones de la Entidad son parametrizados en el sistema de control de acceso.

- ✓ Todos los colaboradores que se les haya asignado carné deberán portarlo al interior de las instalaciones de la Entidad, el cual los acredita como tal; este carné expira al momento de terminado el contrato con el empleado y debe ser entregado al Analista de Contratación.

- ✓ Toda persona externa que pretenda acceder a las instalaciones de VISIONAMOS debe ser identificada a través del video-citófono y ser autorizada desde la Recepción.

- ✓ No se permitirá el acceso de personal externo a la entidad en horarios no habituales.

- ✓ Debe ser controlado el ingreso de: vendedores, cobradores, promotores y visitas particulares; ya que esto puede entorpecer la actividad laboral del personal y puede afectar su productividad, por lo tanto, es necesario solicitar la autorización al Líder Administrativo y/o Subgerentes.

- ✓ En la recepción se deberá mantener un estricto control sobre la entrada y salida de los visitantes.

- ✓ Todos los visitantes deben entregar a la Secretaria de Gerencia un documento de identificación para la entrega del carné de visitante, el cual deberá portar en un lugar visible mientras permanezca en las instalaciones de la Entidad.

- ✓ Cuando un colaborador de VISIONAMOS programe reuniones y/o capacitaciones en las instalaciones de la Entidad con un número superior a diez (10) personas externas a esta, debe informar por correo electrónico como mínimo con un (1) día de anticipación a la Secretaria de Gerencia, el listado de los asistentes con el número de su respectiva identificación e información básica de los equipos de cómputo que vayan a ingresar cualquiera de ellos (tipo, marca y serial) y el tema de dicha capacitación; esto con el fin de dejar registro del acceso de estos visitantes a las instalaciones.

- ✓ El colaborador responsable de recibir una visita debe recibir la persona en la Recepción y se dirigirá con ella, hacia el espacio que hayan reservado para la reunión o capacitación. Una vez cumplido el objetivo de la reunión y/o capacitación previamente coordinada acompañará nuevamente al visitante hasta la puerta de salida.

- ✓ En caso de que el visitante deba acudir a otra área de la organización, el empleado que lo atiende se responsabiliza de su ingreso y acompañamiento hasta finalizar la tarea.

- ✓ Los visitantes, proveedores, terceros u otros deben permanecer acompañados por el colaborador responsable de la visita.

- ✓ Cuando se trate de visitas en periodos prolongados de tiempo, el colaborador designado para coordinar las actividades deberá supervisar regularmente al visitante.

- ✓ A los visitantes que ingresan equipos a las instalaciones de VISIONAMOS, no se le permitirá el acceso a la red interna (alámbrica e inalámbrica); se le brindará acceso a una red de invitados.

- ✓ El carné de visitantes no requiere de fecha de vencimiento, puesto que estos son de uso interno, continuo y la devolución se realizar luego de finalizada la visita.

- ✓ Cuando un colaborador programe con un Contratistas y/o Proveedores actividades dentro de las instalaciones de VISIONAMOS, este debe solicitar con antelación al proveedor y/o contratista la seguridad social vigente y el colaborador de VISIONAMOS lo debe compartir por medio de correo electrónico al Analista de Seguridad y Salud en el Trabajo quien dará la aprobación y/o negación en caso de que aplique; además debe informar a la secretaria de Gerencia la fecha de la actividad y el nombre de la empresa.

- ✓ Toda persona que se vincule a VISIONAMOS con contrato por prestación de servicios y adelante sus laborales en las instalaciones de este, deberá portar el carné de contratista y este será entregado por el Analista de Contratación.

- ✓ La habilitación de las tarjetas de acceso al centro de cómputo y de comunicaciones estará a cargo del Coordinador de Infraestructura previa solicitud por correo electrónico al Oficial de Seguridad. de la Información. La entrega de forma física la realiza el Analista de Contratación y/ Auxiliar de Gestión de Persona, quien deja evidencia en el FAGH-0302 Entrega de Dotación.

- ✓ Los colaboradores que tienen autorización para ingresar al centro de cómputo y de comunicaciones, lo realizan con una tarjeta de banda magnética con control de acceso.

- ✓ Los colaboradores de la Entidad y/o visitantes que requieran ingresar a las áreas restringidas deben permanecer acompañados por personal autorizado para acceder a ellas.

- ✓ Las tarjetas de control de acceso en blanco para ser utilizadas y las que sean devueltas por los colaboradores al momento del retiro de la Entidad, estarán bajo la custodia del Analista de contratación conservando todas las medidas de seguridad correspondientes.

- ✓ En caso de pérdida de la tarjeta de acceso, el colaborador debe reportar de inmediato por correo electrónico al Coordinador de Infraestructura con copia al Analista de Contratación, con el fin de bloquear los privilegios de acceso asociados. Los costos de reposición de la tarjeta de acceso correrán por cuenta del colaborador por medio de una deducción de nómina, en efectivo y/o trasferencias según al acuerdo que se llegue con el colaborador.

- ✓ Se prohíbe el préstamo de la tarjeta de acceso al centro de cómputo y comunicaciones entre colaboradores o visitantes

- ✓ Las oficinas con cerramientos deberán permanecer cerradas durante la ausencia del colaborador responsable.

- ✓ Los colaboradores responsables de áreas restringidas deberán realizar los controles necesarios para que se cumplan con los mecanismos de control de acceso.

- ✓ Todo: evento o novedad que se presente por incumplimiento de las directrices de administración de instalaciones será manejado a través de un proceso disciplinario.

4.6.POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA.

VISIONAMOS adopta una política de escritorios y pantalla limpia para proteger la información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de esta. También aplica a la protección de cualquier tipo de información, en cualquiera de sus formas y que puede estar contenida en escritorios, puestos de trabajo, computadores portátiles, medios ópticos (Unidades Flash, CD-ROM, DVD-ROM, DVD-RAM), medios magnéticos, documentos en papel y en general cualquier tipo de información que es utilizada por los colaboradores de VISIONAMOS para apoyar la ejecución de sus actividades en la Entidad, así mismo dentro del manual S-SI-M-03-Sistema de gestión de seguridad de la información y Ciberseguridad, numeral 10.2.7 se establecen más lineamientos. Los colaboradores de VISIONAMOS deben cumplir con:

- ✓ Los colaboradores son responsables de bloquear la sesión del equipo en el momento en que se retiren del puesto de trabajo, la cual podrán desbloquear sólo con la clave de cada usuario.

- ✓ Con el propósito de evitar daños, pérdidas, o accesos no autorizados a la información de VISIONAMOS, todos los colaboradores deben mantener la información privada o confidencial bajo llave cuando sus puestos de trabajo se encuentren vacíos o en horas no laborales. Esto incluye: documentos impresos, cds, dvds, dispositivos de almacenamiento USB y medios removibles en caso de tenerlos.

4.6.1. UBICACIÓN DE ESCRITORIOS Y EQUIPOS.

Los sitios de trabajo de los colaboradores de VISIONAMOS deben localizarse en ubicaciones que no queden expuestas al acceso de personas externas, exceptuando la oficina de atención al ciudadano, para este caso en lo posible los monitores deben ubicarse de forma que no puedan ser visualizados por personas externas.

4.6.1.1. ESCRITORIO LIMPIO.

Hace referencia a la protección de los papeles y dispositivos removibles de almacenamiento de información, almacenados y manipulados en los puestos de trabajo, de accesos no autorizados, pérdida o daño de la información. Los colaboradores deben:

- ✓ Siempre que algún colaborador se ausente de su estación de trabajo, debe guardar en un lugar seguro y bajo llave cualquier documento físico, medio magnético u óptico que contenga información de uso interno o secreta.

- ✓ Para colaboradores que están ubicado en zonas de atención al público, al ausentarse de su estación de trabajo, debe guardar también los documentos y medios que contengan información de uso interno o secreta

- ✓ Al finalizar la jornada de trabajo, los colaboradores deben guardar en un lugar seguro los documentos y medios que contengan información de uso interno confidencial y restringida, además bloquear los equipos de cómputo, por ejemplo, bloquear los equipos con sistema operativo Windows con las teclas Windows + L y no solo apagar el monitor

- ✓ La información de uso interno, confidencial y restringida, cuando se imprima se debe retirar inmediatamente de las impresoras.

4.6.1.2. PANTALLAS LIMPIAS.

Se refiere a la protección de los equipos de cómputo, tabletas, portátiles u otros dispositivos mediante un bloqueo de pantalla o desconexión cuando no está en uso.

- ✓ Los colaboradores son responsables de bloquear la sesión del equipo en el momento en que se retiren del puesto de trabajo, la cual podrán desbloquear sólo con la clave de cada usuario.
- ✓ La pantalla de computador o escritorio debe estar libre de archivos o enlaces de acceso a archivos; estos deben ubicarse en las debidas carpetas de almacenamiento.
- ✓ Todos los equipos de cómputo y dispositivos portátiles deben tener aplicado el cierre de sesión por inactividad, definido por el proceso de Gestión de Seguridad de la Información.
- ✓ Siempre que el personal se ausente de su puesto de trabajo debe bloquear todos los equipos y dispositivos que de él dependen y/o utiliza.
- ✓ Al activarse el protector de pantalla debe bloquear la sesión en los equipos de cómputo y dispositivos móviles de VISIONAMOS; este debe activarse después de cinco (5) minutos de inactividad de cualquiera de estos equipos.

4.6.2.EQUIPOS DE REPRODUCCIÓN DE INFORMACIÓN.

Los equipos de reproducción de información: impresoras, fotocopiadoras, escáneres, entre otros, deben estar ubicados en lugares de acceso controlado y cualquier documentación con información clasificada de uso interno o confidencial se debe retirar inmediatamente del equipo y ser puesta en un lugar seguro.

- ✓ Los colaboradores no deben dejar las impresoras desatendidas, al momento de imprimir información confidencial o privada de VISIONAMOS se deben retirar de forma inmediata.

4.7. POLÍTICA COPIAS DE SEGURIDAD - BACKUP.

Las copias de seguridad completas e incrementales protegen y preservan la información de la red corporativa y deben realizarse con regularidad para los registros del sistema, datos de la aplicación y los documentos técnicos que no se reemplazan fácilmente, de alto costo de reemplazo o se consideran críticos.

Los medios de respaldo deben almacenarse en un lugar seguro, geográficamente separado del original y aislado de los peligros ambientales. Los componentes de la red de respaldo, el cableado y las fuentes de alimentación, las piezas de repuesto y la documentación relevante deben almacenarse en un área segura en el sitio, así como en otras ubicaciones corporativas. Las políticas de retención de datos y documentos se establecen para especificar qué registros deben conservarse y durante cuánto tiempo. Todos los departamentos de la compañía son responsables de especificar su gestión de datos, retención de datos, destrucción de datos y requisitos generales de gestión de registros.

- ✓ VISIONAMOS debe respaldar de manera segura los datos, sistemas, bases de datos y otra tecnología de misión crítica para que estén disponibles en caso de una interrupción que afecte sus operaciones diarias y pueda recuperarse lo más rápido posible cuando ocurra un incidente.

- ✓ VISIONAMOS debe definir unos documentos que garanticen en cómo realizar el respaldo de los datos e información de gran importancia para VISIONAMOS

- ✓ Se deben minimizar las interrupciones operativas, al documentar, probar y revisar los procedimientos de Backus.

- ✓ Generar fuentes alternas para la realización de los Backups.

- ✓ Los colaboradores que hacen parte del proceso de respaldo deben tener interiorizado por cada uno de los miembros del equipo con el fin de atender de manera oportuna cada uno de los procedimientos.

NOTA: Para dar cumplimiento a lo dispuesto en esta política se define ver el manual T-IT-M-01-Copias de respaldo / procedimiento T-IT-P-02-Gestionar copias de respaldo)

4.7.1. DEFINICION DE ESTANDRES DE DATOS A RESPALDAR.

- ✓ **BASE DE DATOS:**

- Se debe realizar una copia de las bases de datos de misión crítica más actualizadas con una periodicidad continua, o según la frecuencia de los cambios realizados.
- Las copias de seguridad deben almacenarse en un lugar diferente donde corre la base de datos.
- El administrador de datos principal es responsable de esta actividad.

✓ **DATOS CRITICOS:**

- Tras la definición de dichos datos, estos deben respaldarse de acuerdo a la periodicidad que se determine para un punto de retorno ante una falla.
- Las copias de seguridad deben almacenarse en lugar alterno, sea en una ubicación en la nube o un centro de datos alternos de la compañía o una combinación de las anteriores.
- El Administrador de datos principal es responsable de esta actividad.

✓ **DATOS NO CRITICOS:**

- Los datos clasificados no críticos se deben respaldar según se determine en un plan de recuperación en donde se puedan replicar de manera oportuna.
- Deben tener una periodicidad de respaldo de al menos 2 veces por semana.
- Las copias de seguridad deben almacenarse en lugar alterno, sea en una ubicación en la nube o un centro de datos alternos de la compañía o una combinación de las anteriores.
- El Administrador de datos principal es responsable de esta actividad.

✓ **GENERACIÓN DE COPIAS DE DATOS:** Las copias de seguridad de datos se programarán diaria, semanal y mensualmente, según la naturaleza de la copia de seguridad (Ver el manual T-IT-M-01-Copias de respaldo / procedimiento T-IT-P-02-Gestionar copias de respaldo). Los administradores de datos deben utilizar la tecnología de respaldo de datos aprobada para preparar, programar, ejecutar y verificar los respaldos. Se pueden realizar copias de seguridad en recursos de almacenamiento local, por ejemplo, disco, cinta, RAID o en ubicaciones seguras fuera del sitio, por ejemplo, proveedores de servicios de copia de seguridad de datos en la nube, proveedores de copia de seguridad como servicio, aprobados por la administración de TI.

NOTA: RAID es la sigla para "Redundant Array of Independent Disks". Su definición en español sería "Matriz Redundante de Discos Independientes". Se trata de una tecnología que combina varios discos duros (HD) para formar una única unidad lógica, donde los mismos datos son almacenados en todos los discos (redundancia).

✓ **RECUPERACIÓN DE DATOS:** Se deben establecer, documentar y probar periódicamente procedimientos para la recuperación de los datos como bases de datos y otros activos de información si ocurre un evento disruptivo que requiera la recuperación de esos activos y recursos.

ANEXOS /EJMPLOS

EQUIPO DE BACKUP		
NOMBRE	**CORREO ELECTRÓNICO**	**# CELULAR**
Dario Perez	dperez@visonamos.com	3205678923

ALMACENAMIENTO DE DATOS	
COMPAÑÍA	**MÉTODO**
AWS	Copias automatizadas
Google	Control de versiones

4.8. POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

Se deben establecer procedimientos de seguridad en los acuerdos entre las partes involucradas, que tengan parametrizado el manejo de la información y acceso a cada uno de ellos, según sea su aplicabilidad, con el fin de garantizar su confidencialidad y no divulgación de la información reservada. (para más detalle ver el procedimiento PSGSI-05 Gestionar seguridad en medios e información en tránsito)

- ✓ **ALCANCE DE LA POLITICA:** Todas las personas internas o externas a VISIONAMOS.

- ✓ **¿QUIÉNES LA DEBEN CONOCER?**: Colaboradores, consejo de administración, gerente general, subgerentes, terceros y aliados.

- ✓ **RESPONSABILIDAD DE APLICACIÓN**: Los responsables de esta política en su aplicación, modificación y monitoreo son todos los actores que interactúan con VISIONAMOS que desarrollen una actividad con la compañía y los cuales intervengan en el flujo de información en cualquiera de los medios.
  Este tipo de controles están enfocados para asegurar la confidencialidad de la información en el momento de aplicarlos y así definir mecanismos de contención sobre las redes de información por las cuales circulan datos.

✓ **RIESGOS ASOCIADOS:**

- La exposición de la información a todos los usuarios.
- Pérdida, modificación y eliminación de la información.
- Vulneración de la información debido a no contar con algún modo de protección.
- Robo de la información por falta de protección.

✓ **CONTROLES:**

- Se debe contar con políticas, procedimientos y controles de transferencia de Información, para su segura transferencia por los medios de comunicación: al tener procedimientos establecidos, probados y seguros se disminuye la probabilidad de pérdida de información, además que se garantiza la integridad y confidencialidad.
- Se debe proteger adecuadamente la información incluida en la mensajería electrónica: El correo electrónico, al ser una de las principales herramientas y principal medio para compartir información entre departamentos internos y externos, se debe garantizar que la información enviada sea protegida para garantizar su integridad, disponibilidad y confidencialidad.
- Los acuerdos deben tratar la transferencia segura de información del negocio entre la entidad y las partes externas: Se debe asegurar que, al momento de establecer una relación con un tercero, él conozca las políticas de seguridad y las cumpla, también se debe garantizar que si se requiere acceso a los activos críticos de la entidad se realice por canales que proveen un alto nivel de seguridad y que la comunicación se cifre para evitar la interceptación por personas no autorizadas.
- Transferencia de información. Los mecanismos de transferencia de información se especifican y son definidos por las partes involucradas, ya sean internas o externas, donde muestre los acuerdos y requerimientos que deben ser ejecutados al momento en que se requiera el intercambio de información que cuente con algún tipo de privacidad. Estos mecanismos deben ser evaluados y avalados por el área de tecnología para garantizar su funcionalidad, confidencialidad y seguridad.
- Finalmente, VISIONAMOS debe proveer mecanismos y recursos necesarios que cumplan con las funciones anteriormente descritas, en caso de que la información sea muy sensible se deben aplicar mecanismos de codificación o cifrado de acuerdo con estándares internacionales garantizando su integridad y confidencialidad.

4.9. POLÍTICA DE DESARROLLO SEGURO LA ENTIDAD:

Todo desarrollo de software debe cumplir con los criterios de seguridad y calidad de la información. Criterios de seguridad:

- ✓ CONFIDENCIALIDAD: Hace referencia a la protección de información cuya divulgación no está autorizada. Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- ✓ INTEGRIDAD: La información debe ser precisa, coherente y completa desde su creación hasta su destrucción. Propiedad de salvaguardar la exactitud y estado completo de los activos.
- ✓ DISPONIBILIDAD: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso. Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada

Adicionalmente desde su diseño los desarrollados en las aplicaciones deben incorporar elementos de apoyo que hacen parte de las Normas de Seguridad aplicables a la industria y se debe realizar verificación de aplicación de los requisitos de seguridad establecidos en OWASP Top 10.

En el caso de aplicaciones que manejan datos de tarjetas de crédito de los clientes, se debe dar cumplimiento al estándar PCI DSS el cual prohíbe el almacenamiento de números de identificación personal y datos CVV2, validar que esta exigencia no esté desactualizada y su transmisión con cifrado y su visualización mediante enmascaramiento.

Tales requisitos de seguridad de PCI DSS pueden ser validados a través de análisis de código fuente.
Desde la perspectiva funcional, la validación de los requerimientos de seguridad es el principal objetivo de las pruebas de seguridad que deben ser incorporadas desde el mismo diseño de las aplicaciones.

Los requisitos funcionales de seguridad, las normas aplicables, las políticas y reglamentos deben considerar la necesidad de evaluar los controles de seguridad, así como tener el control de la funcionalidad de las aplicaciones.

Desde la perspectiva de gestión del riesgo debe ser objeto de las aplicaciones evaluar y considerar los riesgos dentro de los requerimientos de seguridad, realizando pruebas para validar comportamientos inesperados.

Ejemplos de requerimientos donde se indique lo que "no se debería hacer" (negativo) son los siguientes:

- ✓ La aplicación no debería permitir que la data sea alterada o destruida.
- ✓ La aplicación no debería ser comprometida o mal usada por un usuario malicioso para transacciones financieras no Autorizadas.
- ✓ Garantizar durante el diseño y desarrollo de las aplicaciones que los procesos asociados a esta puedan contar con mecanismos que permitan tener disponibilidad permanente en caso de una caída o falla técnica.
- ✓ Tener gestión administrativa para realizar procedimientos de almacenamiento externo y copias de seguridad de las aplicaciones.
- ✓ Que la información no sea expuesta de alguna manera para evitar alguna vulnerabilidad.

- ✓ **OBJETIVO:** Establecer las condiciones y vigilar que el desarrollo y mantenimiento llevado a cabo, tanto internamente como por proveedores externos de VISIONAMOS, cumpla con buenas prácticas para el desarrollo seguro, además de establecer los criterios de seguridad que deben ser considerados en todas las etapas del desarrollo.

- ✓ **ALCANCE.** Esta política se aplica a todo el software desarrollado para VISIONAMOS. La política da cubrimiento a todo el personal de VISIONAMOS que haga parte de desarrollos, actualizaciones e instalaciones de software.
- ✓ **NIVELES DE ACCESO:** El nivel de acceso a esta política es de carácter confidencial y está orientado a todos los empleados de la Compañía, especialmente aquellos que hacen parte del Equipo de Desarrollo y proveedores externos que tienen que ver concretamente con el desarrollo de nuevos productos o funcionalidades en las aplicaciones existentes.

- ✓ **GENERALIDADES:** El macroproceso de Gestión de Soluciones tecnológicas son los responsables de planificar, desarrollar y ejecutar las actividades relacionadas con el desarrollo, actualizaciones e instalaciones de software. Además, debe planificar la ejecución de pruebas funcionales y de seguridad de los sistemas nuevos o modificados antes de ejecutar la instalación en los servidores de producción.

- ✓ **NORMAS DE SEGURIDAD PARA TODO EL PERSONAL INTERNO Y TERCEROS:**

- Se debe estandarizar el ciclo de vida, los criterios de seguridad y de calidad en el desarrollo de software.

- Toda modificación de software crítico bien sea por actualizaciones o modificaciones, debe ser analizada previamente en ambientes independientes de desarrollo y prueba, con el objetivo de identificar y analizar los riesgos de seguridad que acarrea dicha modificación.
- Se deben planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y pos-instalación, y criterios de aceptación del cambio.
- Para propósitos de desarrollo y pruebas de software, se deben generar datos de prueba distintos a los que se encuentran en el ambiente de producción.
- Los desarrolladores de VISIONAMOS y terceros, no deben tener acceso a información de producción que contenga datos sensibles.
- Se debe establecer un acuerdo previo con los terceros, que resguarde la propiedad intelectual y asegure los niveles de confidencialidad de la información manejada en el proyecto.

✓ **NORMAS DE SEGURIDAD PARA LA GESTIÓN DE VULNERABILIDADES:**

- Se 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.
- Se debe establecer un plan de actualización para el software que es desarrollado o se utiliza en la Entidad, asegurando que las últimas versiones y parches sean instalados lo antes posible, con el fin de evitar que alguna vulnerabilidad sea explotada.

✓ **NORMAS DE SEGURIDAD PARA LA DOCUMENTACIÓN DE SOFTWARE:**

- El proceso de Desarrollo de Software debe contar con un repositorio de metadatos, y deben mantener una descripción actualizada de las definiciones de datos.
- Si el desarrollador incluye comentarios en el programa fuente, estos no deben divulgar información de configuración innecesaria.
- Todo sistema desarrollado por VISIONAMOS debe generar el protocolo de las condiciones de autenticación a la aplicación, el cual debe ser revisado y aprobado por el equipo de seguridad de la información.

La documentación de los desarrollos debe:

- Generarse durante el ciclo de vida de desarrollo y no postergar esta hasta el final.
- Ser revisada por los usuarios finales del sistema en desarrollo.

- Actualizarse si el programa cambia alguna de sus funcionalidades.
- Almacenarse en un sitio centralizado o servidor administrado por el director del Área de Desarrollo o de Infraestructura o quien estos definan para tal fin.

✓ **NORMAS DE SEGURIDAD PARA PROYECTOS DE DESARROLLO:** Como parte de las actividades a realizar en esta fase de un proyecto de desarrollo, se deben describir los requerimientos no funcionales que tienen relación con la seguridad de la información y que deben ser cubiertos en el nuevo producto o la funcionalidad a desarrollar (Para esto se tiene establecido el procedimiento PGEGP-01 Gestión de Proyectos)

✓ **NORMAS DE SEGURIDAD PARA LA ESPECIFICACINES DE REQUERIMIENTOS:** Durante el análisis de factibilidad de los requerimientos, se debe considerar el nivel de criticidad del nuevo producto o funcionalidad, además del nivel de protección de seguridad que requerirán los datos y las aplicaciones que lo compongan. Los requerimientos de seguridad deben ser compatibles con lo que se establece en las demás políticas de seguridad de la información de VISIONAMOS.

- **NORMAS DE SEGURIDAD PARA EL DISEÑO DEL SISTEMA:** El nivel de confidencialidad de todos los elementos que componen el software debe ser definido teniendo en cuenta la criticidad de los datos.

  Si se requiere el uso de cifrado de datos, éste debe ceñirse a los lineamientos descritos en la Política de Criptografía o Cifrado de la Información.

  Si se utiliza un sistema gestor de bases de datos, se deben emplear las herramientas de seguridad necesarias para garantizar el nivel de protección adecuado.

  Todos los programas críticos deben incluir la generación de registros de auditoría, considerando como mínimo la identidad del usuario que lee borra, escribe, o actualiza, el tipo de evento, la fecha y hora del evento. Estos registros deben ser protegidos contra la manipulación no autorizada.

  En la etapa de diseño se debe proyectar el rendimiento esperado, especialmente cuando se trata de un nuevo producto, con el objetivo de no sobredimensionar los recursos necesarios para el funcionamiento del sistema: ancho de banda, RAM, recursos del servidor, etc.

- **NORMAS DE SEGURIDAD PARA LA CODIFICACIÓN Y PRUEBAS:** No está permitido modificar programas sin que quede registrado o documentado el cambio (Para la gestión de cambios ver el procedimiento PMGT-06 Gestionar cambios tecnológicos). En caso de requerirse la implementación de un cambio, este debe ceñirse a los lineamientos descritos en el procedimiento de control de cambios.

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

  En lo posible, las pruebas del sistema deben incluir: instalación, volumen, stress, rendimiento, almacenamiento, configuración, funcionalidad, seguridad y recuperación ante errores.

  En lo posible, las pruebas deben ser realizadas en forma automática, almacenando criterios y datos de pruebas en archivos, para permitir la verificación rápida y repetitiva.

✓ **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, por ejemplo: un servidor.
- 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 la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como tipos de datos, rangos válidos y longitud, entre otros.
- 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.

✓ **CONTROLES PARA LA AUTENTICACIÓN EN LOS SISTEMA DE INFORMACIÓN:**

- Realizar los controles de autenticación en un sistema confiable, por ejemplo, un servidor.
- Si la aplicación administra un almacenamiento de credenciales, asegurar que únicamente se almacena el hash de las contraseñas.

✓ **GESTIÓN DE SESIONES:**

- Realizar la creación de identificadores de sesión en un sistema en el cual se confíe, por ejemplo: el servidor.
- Garantizar la existencia de opciones de desconexión o cierre de sesión de los aplicativos (logout) que permita terminar completamente con la conexión asociada.
- No exponer los identificadores de sesión en URL, mensajes de error ni logs, y no transmitirlos como parámetros.
- Asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
- Asegurar que la sesión expire después de cierto tiempo
- No permitir la apertura de sesiones simultáneas con el mismo usuario.

Se debe asegurar el manejo de operaciones sensibles en los aplicativos desarrollados, permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación. Todas las funciones de criptografía de las aplicaciones desarrolladas deben ser implementadas en sistemas confiables, por ejemplo: el servidor.

✓ **GESTIÓN DE SESIONES:**

- Garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios. Los mensajes de error deben ser genéricos.
- Liberar espacio en memoria cuando ocurra una condición de error.

✓ **MANEJO DE ARCHIVOS:**

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

✓ **ESTABLECIMIENTO DE CONEXIONES A LAS BASES DE DATOS (BD):**

- 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.
- Se debe remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
- Se deben desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos

transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y garantizar que dichos archivos sólo tengan privilegios de lectura.

- No se debe incluir en parámetros, nombres de directorios o rutas de archivos. En su lugar, se deben utilizar índices que internamente se asocien a directorios o rutas predefinidas
- Se debe liberar la memoria previa a la salida de una función y de todos los puntos de finalización de la aplicación.
- Se debe garantizar la protección del código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
- No se debe permitir que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

✓ **NORMAS DE SEGURIDAD PARA LA IMPLEMENTACIÓN:**

- Se debe velar por la implementación de los controles de seguridad al mismo tiempo que la implementación de los componentes, funciones o módulos a los cuales controla.
- Se debe efectuar sintonía o ajuste (tuning) de los controles establecidos en la fase de diseño.
- Las aplicaciones deberán contar con un sistema de autenticación de usuario, que mínimo exija nombre de usuario y contraseña. Además, en los casos que la aplicación esté expuesta a internet, debe implementarse la validación de captcha.
- Las aplicaciones deben contar con manejo de diferentes roles con permisos de acceso y operaciones asociados a estos.

✓ **NORMAS DE SEGURIDAD PARA LA POST IMPLEMENTACIÓN:**

- Se debe revisar y auditar la existencia de los controles de seguridad definidos en la etapa de diseño. Al menos una vez cada año, se debe realizar un escaneo de las aplicaciones más recientes puestas en producción, en busca de vulnerabilidades, manteniendo un registro de los resultados y las acciones correctivas tomadas.

4.10. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN- RELACIÓN CON LOS PROVEEDORES.

El objetivo de la presente política es mantener la seguridad de los activos de información que deban ser accedidos por los proveedores.

Su alcance son todos los activos de información que deban ser accedidos por los proveedores. Las políticas relacionadas a este numeral son *Política de control de acceso definido en el numeral 4.3* y *Política de control de acceso físico definido en el numeral 4.5 de este documento.*

VISIONAMOS debe:

- Identificar todos los proveedores de servicios y/o productos que requieran el acceso tanto físico como lógico a los activos de información. (PSGSI-02 Gestionar Acceso a Recursos Informáticos) Un manejo inadecuado de la seguridad de la información en las relaciones con los proveedores puede poner en riesgo la imagen de VISIONAMOS ante la pérdida, robo, acceso no autorizado o divulgación no autorizada de la información.

- Contar con un proceso para identificar los proveedores (Ver el procedimiento PAFCO-01 Selección proveedores y compras), que incluya el tipo de información que deben acceder y los requisitos de seguridad mínimos para cada tipo de activo de información. La información recabada mediante este procedimiento servirá de base para establecer la relación formal con los proveedores, los contratos y acuerdos de niveles de servicios que deben existir para cada proveedor.

- Establecer formalmente, en los contratos y acuerdos, las obligaciones de ambas partes (VISIONAMOS y el proveedor) con relación a la seguridad de la información. Así mismo, se debe establecer por escrito, la posibilidad de derecho a auditar los procesos y controles del proveedor de productos y/o servicios.

- Considerar la gestión de incidentes de seguridad de la información asociada al acceso a los activos de información por parte de los proveedores. Los incidentes de seguridad de la información deben ser gestionados según lo acordado en el procedimiento PSGSI-04 Gestionar Incidentes de Seguridad y Ciberseguridad.

5. SANCIONES.

Las políticas en VISIONAMOS son de obligatorio cumplimiento; el incumplimiento de alguna de las políticas, controles o procedimientos definidos por la Entidad, en pro de la mejora continua del Sistema de Seguridad de la Información por parte de un colaborador ó tercero que pueda comprometer la integridad de los activos, generará procesos disciplinarios o penales, según la gravedad del incidente presentado.

El no cumplir estas políticas se refiere a la omisión, alteración, no ejecución o manera de no contribuir con la integridad, confidencialidad y disponibilidad de los activos de VISIONAMOS, dado que esto puede comprometer tanto la seguridad como las normas legales y regulatorias.

La aplicación de alguna sanción está sujeta a una investigación formal, en la que se determinen las evidencias del incidente. Dicha validación podría ejecutarse por un externo de VISIONAMOS según sea su nivel de gravedad y de allí se determinará la responsabilidad del implicado en dicha falta. Las sanciones ya deben ser definidas por los directivos de VISIONAMOS y dado el caso se tenga una connotación adicional por alguna entidad externa.

Por lo tanto, el incumplimiento de las políticas aquí estipuladas está sujeto a la aplicación de procesos de acciones disciplinarias que puede conllevar a una sanción de acuerdo con lo escrito en el Reglamento Interno De Trabajo y/o la aplicación de las leyes vigentes en temas de Seguridad de la Información, protección de datos y derechos intelectuales.

El incumplimiento de esta política de seguridad y privacidad de la información traerá consigo las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

6. NOVEDADES Y ACTUALIZACIONES

FECHA	NATURALEZA DEL CAMBIO	ELABORÓ (Nombre/Cargo)	REVISÓ Y APROBÓ (Nombre/Cargo)
9-DIC-2022	Creación del documento (Req 48)	Daniel Londoño /Oficial de Seguridad de la Información	Oscar Martinez / Subgerente del SBPV