Contenido

1. INTRODUCCION

VIDA identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la entidad, razón por la cual es necesario que la empresa establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Este documento describe las políticas y normas de seguridad de la información definidas por VIDA.

Para la elaboración del mismo, se toman como base las leyes y demás regulaciones aplicables, la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013.

Las políticas incluidas en este manual se constituyen como parte fundamental del sistema de gestión de seguridad de la información de VIDA y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.
La seguridad de la información es una prioridad para VIDA y por tanto es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

2. OBJETIVO

El objetivo de este documento es establecer las políticas en seguridad de la información de VIDA, con el fin de regular la gestión de la seguridad de la información al interior de la entidad.

3. ALCANCE

Las políticas de seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, colaboradores y terceros que laboren o tengan relación con VIDA, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

4. DEFINICIONES

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la empresa y, en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: es u documento en los que los colaboradores de VIDA o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la empresa, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Autenticación: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Capacity Planning: es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

Centros de cableado: son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo: es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe

cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.
Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye policías, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Custodio del activo de información: es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

Derechos de Autor: es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Equipo de cómputo: dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Guías de clasificación de la información: directrices para catalogar la información de la entidad y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información

Hacking ético: es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Integridad: es la protección de la exactitud y estado completo de los activos.

Inventario de activos de información: es una lista ordenada y documentada de los activos de información pertenecientes a la empresa.

Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Medio removible: es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

Perfiles de usuario: son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Propiedad intelectual: es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Propietario de la información: es la unidad organizacional o proceso donde se crean los activos de información.

Recursos tecnológicos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de VIDA.

Registros de Auditoría: son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de la empresa. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

Responsable por el activo de información: es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

SGSI: Sistema de Gestión de Seguridad de la Información. **Sistema de información:** es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por VIDA o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Sistemas de control ambiental: son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

Software malicioso: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.
Terceros: todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

Vulnerabilidades: son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la empresa (amenazas), las cuales se constituyen en fuentes de riesgo.

5. POLÍTICA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN

Vida	POLÍTICA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Dirección de VIDA tomando en cuenta su misión, el análisis de contexto, las partes interesadas, la satisfacción del cliente, la mejora continua y en apoyo a su Dirección estratégica, define la siguiente política de seguridad de la información:

Nuestra política de Seguridad de la Información establece los lineamientos que permiten proteger la información de VIDA a través de acciones de gestión de la seguridad de la información teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad y de mejora continua alineados con el contexto de direccionamiento estratégico y de gestión del riesgo con el fin de asegurar el cumplimiento de la integridad, no repudio, disponibilidad, legalidad y confidencialidad de la información.

VIDA, para el cumplimiento de su misión, visión, objetivos estratégicos y alineados a sus valores corporativos, establece la función de Seguridad de la Información en nuestra empresa, con el objetivo de:

- Mantener la confianza de los socios y otras partes interesadas y el compromiso de todos los funcionarios de la organización respecto del correcto manejo y protección de la información que es gestionada y resguardada en VIDA
- Identificar e implementar las tecnologías necesarias para fortalecer la función de la seguridad de la información.
- Implementar el Sistema de Gestión de Seguridad de la Información.
- Proteger la información y los activos tecnológicos de la Institución.
- Asegurar la identificación y gestión de los riegos a los cuales se expone los activos de información de la organización.
- Cumplir con los principios de seguridad de la información: disponibilidad, integridad y confidencialidad.
- Atender las necesidades para el cumplimiento de la función administrativa.
- Proteger la información y los activos tecnológicos de la organización
- Dar un marco para establecer los objetivos de seguridad de la información de la organización
- Concientizar a los funcionarios, proveedores y otras partes interesadas de la organización sobre el uso adecuado de los activos de información puestos a su disposición para la realización de las funciones y actividades diarias.

Esta Política de Seguridad de la Información aplica a toda la organización, sus funcionarios y proveedores, que tengan acceso a información a través de los documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación de la organización.

GUZMÁN GONZÁLEZ

GERENTE DE SISTEMAS

23.5.17

6. COMPROMISO DE LA DIRECCION

La Dirección de VIDA aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad.

La Dirección demuestra su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este manual a todos los colaboradores de la empresa.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- La verificación del cumplimiento de las políticas aquí mencionadas.

7. SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los colaboradores, personal externo y proveedores de VIDA.

Por tal razón, es necesario que las violaciones a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información.

Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan. Ver Procedimiento "VIDA_7_PTO_12_Sanciones Disciplinarias".

8. POLÍTICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

8.1. POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACION

VIDA establecerá un esquema de seguridad de la información en donde existan roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información. Esto se establece en el Manual de Funciones.

8.2. POLITICA PARA USO DE DISPOSITIVOS MOVILES

VIDA proveerá las condiciones para el manejo de los dispositivos móviles empresariales (notebooks y teléfonos inteligentes al personal que lo requiera) que hagan uso de servicios de la empresa. Así mismo, velará porque los colaboradores hagan un uso responsable de los servicios y equipos proporcionados por la organización.

8.2.1. Normas para uso de dispositivos móviles

Normas dirigidas a: TODOS LOS USUARIOS

- Deben evitar usar los dispositivos móviles empresariales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- Se recuerda que no se puede modificar las configuraciones de seguridad de los dispositivos móviles empresariales
- Se recuerda que no se puede instalar programas no autorizados o que atenten contra las buenas costumbres. Sitios web autorizados están detallados en la Lista Blanca por área.
- Deben evitar conectar los dispositivos móviles empresariales asignados cualquier red o computador público, de hoteles o cibercafé, entre otros.
- Debe evitar almacenar videos, fotografías o información personal en los dispositivos móviles empresariales asignados
- Dispositivos personales con cuentas de emails de VIDA deben contar con Autenticación de cada dispositivo.
- No se realizan respaldos de dispositivos móviles, por este motivo no debe almacenarse información de forma permanente en los mismos. La información debe almacenarse en los repositorios definidos.

9. POLÍTICAS DE SEGURIDAD DEL PERSONAL

9.1. POLÍTICA RELACIONADA CON LA VINCULACIÓN DE COLABORADORES

VIDA reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos y, con el interés de contar con el personal mejor calificado, garantizará que la vinculación de nuevos colaboradores se realizará siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los colaboradores en sus cargos.

9.1.1. Normas relacionadas con la vinculación de colaboradores

Normas dirigidas a la función que realiza la selección del personal

- Debe realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en VIDA, antes de su vinculación definitiva.

- Debe certificar que los colaboradores de la empresa firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

Normas dirigidas a: DIRECCIÓN

- VIDA debe verificar la existencia de Acuerdos y/o Cláusulas de Confidencialidad y de la documentación de Aceptación de Políticas para el personal provisto por terceras partes, antes de otorgar acceso a la información de VIDA.

9.2. POLÍTICA APLICABLE DURANTE LA VINCULACION DE COLABORADORES Y PERSONAL PROVISTO POR TERCEROS

VIDA en su interés por proteger su información y los recursos de procesamiento de la misma demostrará el compromiso de la Dirección en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las Políticas de seguridad de la información de la empresa.

Todos los colaboradores de VIDA deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la organización.

9.2.1. Normas aplicables durante la vinculación de colaboradores y personal provisto por terceros

Normas dirigidas a: DIRECCION

- Debe demostrar su compromiso con la seguridad de la información por medio de su aprobación de las políticas, normas y demás lineamientos que desee establecer la empresa.

- Debe promover la importancia de la seguridad de la información entre los colaboradores de VIDA y el personal provisto por terceras partes, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares para la seguridad de la información establecidos.

- Debe definir y establecer el proceso disciplinario o incluir en el proceso disciplinario existente en la empresa, el tratamiento de las faltas de cumplimiento a las políticas de seguridad o los incidentes de seguridad que lo ameriten.

- Debe aplicar el proceso disciplinario de la empresa cuando se identifiquen violaciones o incumplimientos a las políticas de seguridad de la información.

- Debe diseñar y ejecutar de manera permanente un programa de concienciación en seguridad de la información, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma.

- Debe capacitar y entrenar a los colaboradores de VIDA en el programa de concienciación en seguridad de la información para evitar posibles riesgos de seguridad.

- Ver proceso disciplinario en el manual de controles M2, punto 7.2.3

Normas dirigidas a: TODOS LOS USUARIOS

- Los colaboradores y personal provisto por terceras partes que por sus funciones hagan uso de la información de VIDA, deben dar cumplimiento a las políticas, normas y procedimientos de seguridad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.

9.3. POLÍTICA DE DESVINCULACIÓN, LICENCIAS, O CAMBIO DE LABORES DE LOS COLABORADORES Y PERSONAL PROVISTO POR TERCEROS

VIDA asegurará que sus colaboradores y el personal provisto por terceros serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

9.3.1. Normas para la desvinculación, licencias o cambios de labores de los colaboradores y personal provisto por terceros

Normas dirigidas a: Gerente de Sistemas

- Todas las desvinculaciones implican la inmediata remoción de permiso de accesos y bloqueo de contraseñas existentes en un plazo no mayor a 12 horas desde la desvinculación efectiva. Que deberá ser comunicada al área encargada de remoción de accesos vía correo electrónico.

- Para el caso de licencias a priori no se establece necesidad de restricción de accesos o cambios en permisos dado que continúa en efecto el contrato de confidencialidad durante la ausencia del colaborador. Nota: se re direccionar los correos a las personas reemplazantes.

- Para casos de cambio de puesto, se realiza la modificación de credenciales de acceso.

10. POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

10.1. POLÍTICA DE RESPONSABILIDAD POR LOS ACTIVOS

VIDA como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos, entre otros) propiedad de VIDA, son activos de la empresa y se proporcionan a los colaboradores y terceros autorizados, para cumplir con los propósitos del negocio.

Toda la información sensible de VIDA, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte por el Oficial de SGSI. Los responsables del activo deberán llevar un control y actualización periódica del inventario del mismo.

10.1.1. Normas de responsabilidad por los activos

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- La Dirección conjuntamente con el comité de SI de VIDA, deben actuar como propietarios de la información física y electrónica de la organización, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.

- Deben generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo las indicaciones de las guías de clasificación de la información; así mismo, deben mantener actualizado el inventario de sus activos de información.

- Deben monitorear periódicamente anualmente la validez de los usuarios y sus perfiles de acceso a la información. Si algún usuario presenta dificultad de acceso se releva la validez de la totalidad de los usuarios y su perfil de acceso.

- Deben ser conscientes que los recursos de procesamiento de información de la empresa, se encuentran sujetos a auditorías por parte del Oficial de SGSI y a revisiones de cumplimiento por parte del Comité de SI.

Normas dirigidas a: Gerente de Sistemas

- Es el responsable de los activos de información correspondientes a la plataforma tecnológica de VIDA y, en consecuencia, debe asegurar su apropiada operación y administración.

- El Gerente de Sistemas en conjunto con el Comité de SI, son quienes deben autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica de VIDA.

- Debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.

- Es responsable de preparar las estaciones de trabajo fijas y/o portátiles de los colaboradores y de hacer entrega de las mismas.

- Es responsable de recibir los equipos de trabajo fijo y/o portátil para su reasignación o disposición final, y generar copias de seguridad de la información de los colaboradores que se retiran o cambian de labores, cuando les es formalmente solicitado.

Normas dirigidas a: Comité de SI

- Debe realizar un análisis de riesgos de seguridad de manera periódica, sobre los procesos de VIDA.

- Debe definir las condiciones de uso y protección de los activos de información, tanto los tecnológicos como aquellos que no lo son.

- Debe realizar revisiones periódicas de los recursos de la plataforma tecnológica y los sistemas de información de la empresa.

- Debe autorizar a sus colaboradores el uso de los recursos tecnológicos, previamente preparados por la Gerencia de Sistemas.

Normas dirigidas a: TODOS LOS USUARIOS

- Los recursos tecnológicos de VIDA, deben ser utilizados de forma ética y en cumplimiento de las leyes vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la empresa.

- Los colaboradores no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica de VIDA.

Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.

10.2. POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

VIDA definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad, y generará una guía de Clasificación de la Información (registro de Gestión de Activos) para que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección.

Toda la información de VIDA debe ser identificada, clasificada y documentada de acuerdo con las guías de Clasificación de la Información establecidas por el Comité de Seguridad de la Información.

Una vez clasificada la información, VIDA proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte de los colaboradores de la empresa y personal provisto por terceras partes que se encuentre autorizado y requiera de ella para la ejecución de sus actividades.

10.2.1. Normas para la clasificación y manejo de la información

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACION

- Debe recomendar los niveles de clasificación de la información y la guía de clasificación de la Información de VIDA para que sean aprobados por la Dirección.

- Debe definir los niveles de clasificación de la información para VIDA y, posteriormente generar la guía de clasificación de la Información.

Normas dirigidas a: Gerente de Sistemas

- Debe efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.
- Forma de intercambio de información con otras organizaciones (incluyendo la forma de identificar la clasificación de la información y la forma de interpretar etiquetas de clasificación de otras organizaciones):
    - Garino (facturación electrónica): envío de recibos al proveedor por medio electrónico con firma electrónica
    - Nodum (software contable): administración y gestión de la información de VIDA en las instalaciones de VIDA

Normas dirigidas a: TODOS LOS USUARIOS

- Deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíes faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.

- Tanto los colaboradores como el personal provisto por terceras partes deben asegurarse que, en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo

10.3. POLÍTICA DE USO DE PERIFERICOS Y MEDIOS DE ALMACENAMIENTO

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de VIDA será reglamentado por el Gerente de Sistemas junto con el Comité de SI, considerando las labores realizadas por los colaboradores y su necesidad de uso.

10.3.1. Normas uso de periféricos y medios de almacenamiento

Normas dirigidas a: Gerente de Sistemas

- Deben establecer las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica de VIDA.

- Debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la empresa, de acuerdo con los lineamientos y condiciones establecidas.

- Debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento de la empresa, ya sea cuando son dados de baja o re-asignados a un nuevo usuario.

Normas dirigidas a: Oficial de SGSI

- Debe autorizar el uso de periféricos o medios de almacenamiento en la plataforma tecnológica de la empresa de acuerdo con el perfil del cargo del funcionario solicitante.

Normas dirigidas a: TODOS LOS USUARIOS

Los colaboradores y personal provisto por terceras partes no deben utilizar medios de almacenamiento en la plataforma tecnológica de VIDA no autorizados.

11. POLÍTICAS DE CONTROL DE ACCESO

11.1. POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED

La Gerencia de VIDA, como responsables de las redes de datos y los recursos de red de la empresa, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

11.1.1. Normas de acceso a redes y recursos de red

Normas dirigidas a: GERENCIA DE SISTEMAS

- Debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de VIDA:
    - Cada empleado dispone de su perfil en la red que le permite acceder a los archivos que debe manejar
    - En caso de dudas sobre el perfil se consulta al encargado del área
    - La autorización es realizada por el área de Sistemas
- Debe asegurar que las redes inalámbricas de la empresa cuenten con métodos de autenticación que evite accesos no autorizados.
- La Gerencia de Sistemas debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de VIDA, así como velar por la aceptación de

las responsabilidades de dichos terceros, cuando corresponda. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

- Debe autorizar la creación o modificación de las cuentas de acceso a las redes o recursos de red de VIDA.
- Debe verificar periódicamente los controles de acceso para los usuarios provistos por terceras partes, con el fin de revisar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.

Normas dirigidas a: TODOS LOS USUARIOS

- Los colaboradores de VIDA y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de VIDA, deben contar con las credenciales de acceso (usuario, contraseña e IP) debidamente autorizado y el Acuerdo de Confidencialidad firmado previamente.
- Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la empresa deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

11.2. POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

11.2.1. Normas de administración de acceso de usuarios

Normas dirigidas a: GERENCIA DE SISTEMAS

- Debe establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la empresa, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario:
  - Creación: se crea un usuario con sus credenciales
  - Modificación: cuando se requiera una modificación, se amplía el alcance de acceso
  - Bloqueo: cuando se está en proceso de despido, se bloquean todos los accesos
  - Eliminación: posterior, al despido, y una vez revisado los archivos se elimina el usuario
- La Gerencia de Sistemas, previa solicitud de los responsables respectivos de los solicitantes de las cuentas de usuario y aprobación tanto de los propietarios de los sistemas de información, debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento anterior.
- Debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los colaboradores se
  - Desvinculan: cambio de contraseñas y se espera de un período de un mes para eliminar todo tipo de cuentea
  - Toman licencias y vacaciones: se redirigen las tareas e informaciones al suplente
  - Cambian de cargo: se cambia el perfil de acceso a los nuevos requerimientos del cargo
- Es responsabilidad de la Gerencia de Sistemas definir los perfiles de usuario y autorizar, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.
- Deben verificar y ratificar anualmente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

11.3. POLÍTICA DE RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

- Los usuarios de los recursos tecnológicos y los sistemas de información de VIDA realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

11.3.1. Normas de responsabilidades de acceso de los usuarios

Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información de VIDA deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.
- Los colaboradores no deben compartir sus cuentas de usuario y contraseñas con otros colaboradores o con personal provisto por terceras partes.
- Los colaboradores y personal provisto por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información de la empresa deben acogerse a lineamientos para la configuración de contraseñas implantados por la empresa.

11.4. POLÍTICA DE USO DE ALTOS PRIVILEGIOS Y UTILITARIOS DE ADMINISTRACION

La Gerencia de Sistemas de VIDA velará porque los recursos de la plataforma tecnológica y los servicios de red de la empresa sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dichos plataforma y servicios.

11.4.1. Normas de uso de altos privilegios y utilitarios de administración

Normas dirigidas a: GERENCIA DE SISTEMAS

- La Gerencia de Sistemas debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos colaboradores designados para dichas funciones.
- Debe establecer cuentas personalizadas con altos privilegios para el personal de Sistemas de los recursos tecnológicos, servicios de red y sistemas de información.
- Debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.
- Debe asegurarse que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos sean suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.
- Debe establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.
- Los administradores de los recursos tecnológicos y servicios de red, no tienen acceso a los utilitarios que permiten acceso a los sistemas operativos, firmware o conexión a las bases de datos para pasar por alto la seguridad de los sistemas de información alojados sobre la plataforma tecnológica de VIDA.
- Deben deshabilitar las funcionalidades o servicios no utilizados de los sistemas operativos, el firmware y las bases de datos. Se debe configurar el conjunto mínimo requerido de funcionalidades, servicios y utilitarios.
- La Gerencia de Sistemas debe generar y mantener actualizado un listado de las cuentas administrativas de los recursos de la plataforma tecnológica.

11.5. POLÍTICA DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

La Gerencia de Sistemas como propietaria de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velará por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

Propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, velará porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

11.5.1. Normas de control de acceso a sistemas y aplicativos

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- Deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

Normas dirigidas a: GERENCIA DE SISTEMAS

- Debe establecer un procedimiento para la asignación de accesos a los sistemas y aplicativos de VIDA (ver Manual de Puesto Nuevo y de Cambio de puesto)
- Debe establecer ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.
- Debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios.

Normas dirigidas a: DESARROLLADORES (INTERNOS Y EXTERNOS)

- Deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.
- Deben certificar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.
- Deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.
- Deben asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben habilitar la funcionalidad de recordar campos de contraseñas.
- Deben certificar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.
- Deben, a nivel de los aplicativos, restringir acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.

11.6 POLÍTICAS DE AUTENTICACIÓN SECRETA

a) Mantener en secreto la información de autenticación confidencial, asegurando que no se divulga a otras partes, incluyendo las personas con autoridad
b) Cambiar la información de autenticación secreta cuando haya indicios de su posible compromiso
c) No compartir la información de autenticación secreta del usuario individual;
d) Garantizar una adecuada protección de las contraseñas cuando las mismas son utilizadas como información de autenticación secreta en procedimientos de inicio de sesión automático y luego almacenadas;
e) no utilicen la misma información de autenticación secreta para las propuestas comerciales y no comerciales.

12. POLÍTICAS DE CRIPTOGRAFIA

No aplica al momento a VIDA.

13. POLÍTICAS DE SEGURIDAD FISICA Y MEDIOAMBIENTAL

13.1. POLÍTICA DE AREAS SEGURAS

VIDA proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideras áreas de acceso restringido.

13.1.1. Normas de áreas seguras

Normas dirigidas a: GERENCIA DE SISTEMAS

- Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por colaboradores de la GERENCIA DE SISTEMAS autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha dirección durante su visita al centro de cómputo o los centros de cableado.
- Debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.
- Debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.
- Debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.
- Debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- Debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

Normas dirigidas a: Dirección

- Los directores que se encuentren en áreas restringidas deben velar mediante monitoreo por la efectividad de los controles de acceso físico y equipos de vigilancia implantados en sus áreas.
- Los directores que se encuentren en áreas restringidas deben autorizar cualquier ingreso temporal a sus áreas, evaluando la pertinencia del ingreso; así mismo, deben delegar en personal del área el registro y supervisión de cada ingreso a sus áreas.
- Los directores deben velar porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas solo sean utilizados por los colaboradores autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos no sean transferidos a otros colaboradores de la empresa.

Normas dirigidas a: OFICINA DE RIESGOS

- Debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de VIDA.
- Debe identificar mejoras a los mecanismos implantados y, de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la empresa.
- Debe almacenar y custodiar los registros del sistema de control de acceso a las instalaciones de VIDA.
- Debe certificar la efectividad de los mecanismos de seguridad física y control de acceso al centro de cómputo, centros de cableado y demás áreas de procesamiento de información.
- Debe controlar el ingreso de los visitantes a los centros de cableado que están bajo su custodia.
- Debe cerciorarse de que los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

- con el acompañamiento de la GERENCIA DE SISTEMAS, debe verificar que el cableado se encuentra protegido con el fin de disminuir las intercepciones o daños.

Normas dirigidas a: TODOS LOS USUARIOS

- Los ingresos y egresos de personal a las instalaciones de VIDA deben ser registrados; por consiguiente, los colaboradores y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.
- Los colaboradores deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la empresa; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.
- Aquellos colaboradores o personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.
- Los colaboradores de VIDA y el personal provisto por terceras partes no deben intentar ingresar a áreas a las cuales no tengan autorización.

13.2. POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS EMPRESARIALES

VIDA para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la empresa que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

13.2.1. Normas de seguridad para los equipos empresariales

Normas dirigidas a: GERENCIA DE SISTEMAS

- Debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de VIDA.
- Debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la empresa.
- La GERENCIA DE SISTEMAS, en conjunto con la Coordinación de Recursos Físicos debe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del centro de cómputo y otras áreas de procesamiento de información.
- Debe generar estándares de configuración segura para los equipos de cómputo de los colaboradores de la empresa y configurar dichos equipos acogiendo los estándares generados.
- Debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la empresa y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.
- Debe aislar los equipos de áreas sensibles, como la Dirección de Tesorería para proteger su acceso de los demás colaboradores de la red de la empresa.
- Debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los colaboradores de la empresa, ya sea cuando son dados de baja o cambian de usuario.

Normas dirigidas a: OFICINA DE RIESGOS

- tiene la responsabilidad de incluir dentro del plan anual de auditorías la verificación aleatoria a los equipos de cómputo de todas las dependencias y puntos de atención de la entidad.
- Debe evaluar y analizar los informes de verificación de equipos de cómputo de las diferentes áreas de la empresa, en particular de las áreas sensibles.
- Debe revisar los accesos físicos en horas no hábiles a las áreas donde se procesa información.
- Debe restringir el acceso físico a los equipos de cómputo de áreas donde se procesa información sensible.
- debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos empresariales de las instalaciones de VIDA cuente con la autorización documentada y aprobada previamente por el Coordinador de Recursos Físicos.
- Físicos debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la empresa, posean pólizas de seguro.

Normas dirigidas a: TODOS LOS USUARIOS

- La GERENCIA DE SISTEMAS es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la empresa.
- Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los colaboradores y personal provisto por terceras partes deben acoger las instrucciones técnicas de proporcione la GERENCIA DE SISTEMAS.
- Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad de VIDA el usuario responsable debe informar a la Mesa de Ayuda en donde se atenderá o escalará al interior de la GERENCIA DE SISTEMAS, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.
- La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la empresa, solo puede ser realizado por los colaboradores de la GERENCIA DE SISTEMAS, o personal de terceras partes autorizado por dicha dirección.
- Los colaboradores de la empresa y el personal provisto por terceras partes deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.
- Los colaboradores de VIDA y el personal provisto por terceras partes no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.
- Los equipos de cómputo, bajo ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.
- Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.

Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

En caso de pérdida o robo de un equipo de cómputo de VIDA, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

Los colaboradores de la empresa y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

14. POLITICAS DE SEGURIDAD EN LAS OPERACIONES

14.1. POLÍTICA DE ASIGNACIÓN DE RESPONSABILIDADES OPERATIVAS

La GERENCIA DE SISTEMAS, encargada de la operación y administración de los recursos tecnológicos que apoyan los procesos de VIDA, asignará funciones específicas a sus colaboradores, quienes deben efectuar la operación y administración de dichos recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades. Así mismo, velará por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada y asegurará que los cambios efectuados sobre los recursos tecnológicos, serán adecuadamente controlados y debidamente autorizados.

La GERENCIA DE SISTEMAS proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información de la empresa, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.

14.1.1. Normas de asignación de responsabilidades operativas

Normas dirigidas a: GERENCIA DE SISTEMAS

- Debe efectuar, a través de sus colaboradores, la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de la empresa.

- Debe proporcionar a sus colaboradores manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica de VIDA.

- Debe proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.

- Debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

Normas dirigidas a: OFICINA DE RIESGOS

- Debe emitir concepto y generar recomendaciones acerca de las soluciones de seguridad seleccionadas para la plataforma tecnológica de la empresa.

14.2. POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

VIDA proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus colaboradores y personal provisto por terceras partes frente a los ataques de software malicioso.

14.2.1. Normas de protección frente a software malicioso

Normas dirigidas a: GERENCIA DE SISTEMAS

- Debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de VIDA y los servicios que se ejecutan en la misma.

- Debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.

- Debe certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.

- Debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.

- Debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por la GERENCIA DE SISTEMAS; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.

- Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez,

especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.

- Deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.

- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la Mesa de Ayuda, para que a través de ella, la GERENCIA DE SISTEMAS tome las medidas de control correspondientes.

14.3. POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

VIDA certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo de la GERENCIA DE SISTEMAS, encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

14.3.1. Normas de copias de respaldo de la información

Normas dirigidas a: GERENCIA DE SISTEMAS

- Debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.

- Debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

- Debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.

Debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.

- Debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de la los activos información de la empresa.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Los propietarios de los recursos tecnológicos y sistemas de información deben definir, en conjunto con la GERENCIA DE SISTEMAS, las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.

Normas dirigidas a: TODOS LOS USUARIOS

- Es responsabilidad de los usuarios de la plataforma tecnológica de VIDA identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

14.4. POLÍTICA DE REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y LOS SISTEMAS DE INFORMACIÓN

VIDA realizará monitoreo permanente del uso que dan los colaboradores y el personal provisto por terceras partes a los recursos de la plataforma tecnológica y los sistemas de información de la empresa. Además, velará por la custodia de los registros de auditoria cumpliendo con los periodos de retención establecidos para dichos registros.

La GERENCIA DE SISTEMAS y la Oficina de Riesgos definirán la realización de monitoreo de los registros de auditoria sobre los aplicativos donde se opera los procesos misionales de la empresa. El Comité de revisión de logs mensualmente se reunirá a analizar los resultados del monitoreo efectuado.

14.4.1. Normas de registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información

Normas dirigidas a: GERENCIA DE SISTEMAS Y OFICINA DE RIESGOS

- Debe determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información de VIDA.

- La GERENCIA DE SISTEMAS y la Oficina de Riesgos, a través del Comité de revisión de logs, deben definir de manera mensual cuáles monitoreos se realizarán de los registros de auditoria sobre los aplicativos donde se opera los procesos misionales de la empresa. Así mismo, se deben reunir para analizar los resultados de cada monitoreo efectuado.

- La GERENCIA DE SISTEMAS, a través de sus colaboradores, debe habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar establecidos.

- La GERENCIA DE SISTEMAS debe certificar la integridad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica y los sistemas de información de VIDA. Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.

- La Oficina de Riesgos debe determinar los periodos de retención de los registros (logs) de auditoria de los recursos tecnológicos y los sistemas de información de la empresa.

- La Oficina de Riesgos debe revisar periódicamente los registros de auditoria de la plataforma tecnológica y los sistemas de información con el fin de identificar brechas de seguridad y otras actividades propias del monitoreo.

Normas dirigidas a: DESARROLLADORES (INTERNOS Y EXTERNOS)

- Deben generar registros (logs) de auditoría de las actividades realizadas por los usuarios finales y administradores en los sistemas de información desarrollados. Se deben utilizar controles de integridad sobre dichos registros.

- Deben registrar en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, de acuerdo con las directrices establecidas por la GERENCIA DE SISTEMAS y la Oficina de Riesgos.

- Deben evitar almacenar datos innecesarios de los sistemas construidos en los logs de auditoria que brinden información adicional a la estrictamente requerida.

14.5. POLITICA DE CONTROL AL SOFTWARE OPERATIVO

VIDA, a través de la Gerencia, designará responsables y establecerá procedimientos para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado.

14.5.1. Normas de control al software operativo

Normas dirigidas a: GERENCIA DE SISTEMAS

- Debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente en la empresa.

- Debe asegurarse que el software operativo instalado en la plataforma tecnológica de VIDA cuenta con soporte de los proveedores.

- Debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.

- Debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.

- Debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la empresa.

14.6. POLÍTICA DE GESTIÓN DE VULNERABILIDADES

VIDA, a través de la GERENCIA DE SISTEMAS y la Oficina de Riesgos, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas. Estas dos áreas conforman en Comité de vulnerabilidades encargado de revisar, valorar y gestionar las vulnerabilidades técnicas encontradas.

14.6.1. Normas para la gestión de vulnerabilidades

Normas dirigidas a: OFICINA DE RIESGOS

- Debe adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas.

- Debe generar los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.

Normas dirigidas a: GERENCIA DE SISTEMAS

- Debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.

- Debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.

Normas dirigidas a: GERENCIA DE SISTEMAS Y OFICINA DE RIESGOS

- La GERENCIA DE SISTEMAS y la Oficina de Riesgos, a través del Comité de vulnerabilidades, deben revisar, valorar y gestionar las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación.

15. POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES

15.1. POLÍTICA DE GESTION Y ASEGURAMIENTO DE LAS REDES DE DATOS

VIDA establecerá, a través de la Gerencia de Sistemas, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida de la empresa.

15.1.1. Normas de gestión y aseguramiento de las redes de datos

Normas dirigidas a: GERENCIA DE SISTEMAS

- Debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red de VIDA.
- Debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.
- Debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la empresa.
- Debe identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.
- Debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica de la empresa, acogiendo buenas prácticas de configuración segura.
- Debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos por la empresa en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.
- Debe instalar protección entre las redes internas de VIDA y cualquier red externa, que este fuera de la capacidad de control y administración de la empresa.
- Debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos de VIDA.

15.2. POLÍTICA DE USO DEL CORREO ELECTRONICO

VIDA, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre colaboradores y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

15.2.1. Normas de uso del correo electrónico

Normas dirigidas a: GERENCIA DE SISTEMAS Y OFICINA DE RIESGOS

- Debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.
- Debe diseñar y divulgar las directrices técnicas para el uso de los servicios de correo electrónico.
- Debe proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.
- Debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.
- Debe generar campañas para concientizar tanto a los colaboradores internos, como al personal provisto por terceras partes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

Normas dirigidas a: TODOS LOS USUARIOS

- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario de la empresa o provisto por un tercero, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.

- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de VIDA. El correo institucional no debe ser utilizado para actividades personales.

- Los mensajes y la información contenida en los buzones de correo son propiedad de VIDA y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

- Los usuarios de correo electrónico institucional tienen prohibido el envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los colaboradores de la empresa y el personal provisto por terceras partes.

- No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por VIDA y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

15.3. POLÍTICA DE USO ADECUADO DE INTERNET

VIDA consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la empresa.

15.3.1. Normas de uso adecuado de internet

Normas dirigidas a: GERENCIA DE SISTEMAS

- Debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

- Debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

- Debe monitorear continuamente el canal o canales del servicio de Internet.

- Debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

- Debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.

Normas dirigidas a: OFICINA DE RIESGOS

- Debe generar campañas para concientizar tanto a los colaboradores internos, como al personal provisto por terceras partes, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de Internet.

Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios del servicio de Internet de VIDA deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.

- Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.

- Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Yahoo, Sype, Net2phome y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de VIDA.

- No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y la GERENCIA DE SISTEMAS, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

- No está permitido el intercambio no autorizado de información de propiedad de VIDA, de sus clientes y/o de sus colaboradores, con terceros.

15.4. POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

VIDA asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán Acuerdos de Confidencialidad y/o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio. La empresa propenderá por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de información en medio físico.

15.4.1. Normas de intercambio de información

Normas dirigidas a: Gerencia de Sistemas

- En acompañamiento con la Oficina de Riesgos, debe definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre la empresa y terceras partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir la prohibición de divulgar la información entregada por VIDA a los terceros con quienes se establecen estos acuerdos y la destrucción de dicha información una vez cumpla su cometido.

- Debe establecer en los contratos que se establezcan con terceras partes, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de beneficiarios de la empresa que les ha sido entregada en razón del cumplimiento de los objetivos misionales de VIDA.

Normas dirigidas a: OFICINA DE RIESGOS

- Debe definir y establecer el procedimiento de intercambio de información con los diferentes terceros que, hacen parte de la operación de VIDA, reciben o envían información de los beneficiarios de la empresa, que contemple la utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de la misma.

- Debe velar porque el intercambio de información de VIDA con entidades externas se realice en cumplimiento de las Políticas de seguridad para el intercambio de información aquí descritas, los Acuerdos de Intercambio de Información y el procedimiento definido para dicho intercambio de información.

- Debe autorizar el establecimiento del vínculo de transmisión de información con terceras partes, para que posteriormente las áreas funcionales realicen las actividades de transmisión requeridas en cada caso.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- Deben velar porque la información de VIDA o de sus beneficiarios sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las clausulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.

- Deben asegurar que los datos requeridos de los beneficiarios sólo puedan ser entregada a terceros, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.

- Deben verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.

- Deben autorizar los requerimientos de solicitud/envío de información de VIDA por/a terceras partes, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.

- Deben asegurarse que el Intercambio de información (digital) solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de administración de redes, de acceso lógico y de protección de datos personales de VIDA así como del procedimiento de intercambio de información.

- Deben verificar la destrucción de la información suministrada a los terceros, realizada por ellos una vez esta ha cumplido el cometido por el cual fue enviada.

Normas dirigidas a: Gerencia de Sistemas

- Debe acoger el procedimiento para el intercambio, de información (medios de almacenamiento y documentos) con terceras partes y la adopción de controles a fin de proteger la información sensible contra divulgación, pérdida o modificaciones.

- Debe certificar que todo envió de información física a terceros (documento o medio magnético) utilice únicamente los servicios de transporte o servicios de mensajería autorizados por VIDA, y que estos permitan ejecutar rastreo de las entregas.

Normas dirigidas a: GERENCIA DE SISTEMAS

- Debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

Normas dirigidas a: TERCEROS CON QUIENES SE INTERCAMBIA INFORMACION DE VIDA

- Deben darle manejo adecuado a la información recibida, en cumplimiento de las Políticas de seguridad de la empresa, de las condiciones contractuales establecidas y del Procedimiento de intercambio de información.

- Deben destruir de manera segura la información suministrada, una vez esta cumpla con la función para la cual fue enviada y demostrar la realización de las actividades de destrucción.

Normas dirigidas a: TODOS LOS USUARIOS:

- No deben utilizar el correo electrónico como medio para enviar o recibir información sensible de la empresa o de sus beneficiarios.

- No está permitido el intercambio de información sensible de la empresa por vía telefónica.

16. POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

16.1. POLÍTICA PARA EL ESTABLECIMIENTO DE REQUISITOS DE SEGURIDAD

VIDA asegurará que el software adquirido y desarrollado tanto al interior de la empresa, como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos por la empresa

Las áreas propietarias de sistemas de información, la Gerencias de Sistemas y la Oficina de Riesgos incluirán requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

16.1.1. Normas para el establecimiento de requisitos de seguridad

Normas dirigidas a: PROPIETARIOS DE LOS SISTEMAS DE INFORMACIÓN, GERENCIA DE SISTEMAS Y OFICINA DE RIESGOS

- Todos los sistemas de información o desarrollos de software deben tener un área propietaria dentro de la empresa formalmente asignada.

- La GERENCIA DE SISTEMAS debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.

- Las áreas propietarias de los sistemas de información, en acompañamiento con la GERENCIA DE SISTEMAS y la Oficina de Riesgos deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la información.

- Las áreas propietarias de los sistemas de información deben definir qué información sensible puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.

- La Oficina de Riesgos debe liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.

Normas dirigidas a: DESARROLLADORES (INTERNOS O EXTERNOS)

- Deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.

- Deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.

- Deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.

- Deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.

- Deben asegurar que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.

- Deben utilizar usar los protocolos sugeridos por la GERENCIA DE SISTEMAS y la Oficina de Riesgos en los aplicativos desarrollados.

- Deben certificar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.

16.2. POLÍTICA DE DESARROLLO SEGURO, REALIZACION DE PRUEBAS Y SOPORTE DE LOS SISTEMAS

VIDA velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la empresa.

16.2.1. Normas de desarrollo seguro, realización de pruebas y soporte de los sistemas

Normas dirigidas a: PROPIETARIOS DE LOS SISTEMAS DE INFORMACIÓN

- Son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.

- Deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

Normas dirigidas a: GERENCIA DE SISTEMAS

- Debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.

- Debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de VIDA.

- Debe asegurase que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

- Debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.

- La GERENCIA DE SISTEMAS, a través de sus colaboradores, se debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.

- Debe incluir dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software aplicativo y los sistemas de información de la empresa.

Normas dirigidas a: DESARROLLADORES (INTERNOS O EXTERNOS)

- Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.

- Deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo de VIDA; dicho soporte debe contemplar tiempos de respuesta aceptables.

- Deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

- Deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

- Deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
- Deben asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.

- Deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.

- Deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.

- Deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.

- Deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.

- Deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.

- Deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.

- Deben certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.

- 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 asegurar que dichos archivos solo tengan privilegios de lectura.

- Deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

- Deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

Normas dirigidas a: OFICINA DE RIESGOS

- Debe verificar que las pruebas de seguridad sobre los sistemas de información se realicen de acuerdo con las metodologías definidas, contando con pruebas debidamente documentadas.

16.3. POLÍTICA PARA LA PROTECCION DE LOS DATOS DE PRUEBA

La GERENCIA DE SISTEMAS de VIDA protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción.

16.3.1. Normas para la protección de los datos de prueba

Normas dirigidas a: GERENCIA DE SISTEMAS

- Debe certificar que la información a ser entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción.

- Debe eliminar la información de los ambientes de pruebas, una vez estas han concluido.

17. POLÍTICAS QUE RIGEN DE LA RELACION CON TERCERAS PARTES

17.1. POLÍTICA DE INCLUSION DE CONDICIONES DE SEGURIDAD EN LA RELACIÓN CON TERCERAS PARTES

VIDA establecerá mecanismos de control en sus relaciones con terceras partes, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

Los colaboradores responsables de la realización y/o firma de contratos o convenios con terceras partes se asegurarán de la divulgación de las políticas, normas y procedimientos de seguridad de la información a dichas partes.

17.1.1. Normas de inclusión de condiciones de seguridad en la relación con terceras partes

Normas dirigidas a: GERENCIA DE SISTEMAS, OFICINA ASESORA JURIDICA Y OFICINA DE RIESGOS

- Deben generar un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad de la Información, con los que deben cumplir terceras partes o proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.

- Deben elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con terceras partes. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.

Normas dirigidas a: GERENCIA DE SISTEMAS

- Debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la empresa.

- Debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

- Debe mitigar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica de VIDA.

Normas dirigidas a: OFICINA DE RIESGOS

- Debe evaluar y aprobar los accesos a la información de la empresa requeridos por terceras partes.

- Debe identificar y monitorear los riesgos relacionados con terceras partes o los servicios provistos por ellas, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología o comunicaciones provistos.

Normas dirigidas a: SUPERVISORES DE CONTRATOS CON TERCEROS

- Deben divulgar las políticas, normas y procedimientos de seguridad de la información de VIDA a dichos terceros, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de la misma, por parte de los terceros se realice de manera segura, de acuerdo con las políticas, normas y procedimientos de seguridad de la información.

17.2. POLÍTICA DE GESTION DE LA PRESTACION DE SERVICIOS DE TERCERAS PARTES

VIDA propenderá por mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos con estos. Así mismo, velará por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.

17.2.1. Normas de gestión de la prestación de servicios de terceras partes

Normas dirigidas a: GERENCIA DE SISTEMAS Y OFICINA DE RIESGOS

- La GERENCIA DE SISTEMAS debe verificar en el momento de la conexión y, cuando se considere pertinente, el cumplimiento de las condiciones de conexión de los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la empresa.

- La Gerencia de Tecnologías de la Información y la Oficina de Riesgos deben verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

Normas dirigidas a: OFICINA DE RIESGOS

- Debe monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información de parte de los terceros proveedores de servicios.

- Debe administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.

- Debe verificar que estén establecidos y acordados todos los requisitos pertinentes de SI con los proveedores que puedan acceder, procesar, almacenar, comunicar o proporcionar componentes de la estructura de TI para la información de la organización

- Debe verificar que los acuerdos con proveedores incluyan requisitos para abordar los riesgos de SI asociados con la cadena de suministro de productos y servicios de TI y las comunicaciones.

18. POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

18.1. POLÍTICA PARA EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

VIDA promoverá entre los colaboradores y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio

de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.

De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

La Alta Dirección o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

18.1.1. Normas para el reporte y tratamiento de incidentes de seguridad

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Deben informar a la Oficina de Riesgos, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

Normas dirigidas a: OFICINA DE RIESGOS

- Debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.

- Debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar al Comité de Seguridad de la Información aquellos en los que se considere pertinente.

- Debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su re-ocurrencia.
- Debe, con el apoyo con la GERENCIA DE SISTEMAS y la Secretaría General, crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACION

- Debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

Normas dirigidas a: TODOS LOS USUARIOS

- Es responsabilidad de los colaboradores de VIDA y del personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.

- En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los colaboradores deben notificarlo a la Oficina de Riesgo para que se registre y se le dé el trámite necesario.

19. POLÍTICAS DE INCLUSION DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

19.1. POLÍTICA DE CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD CON CONSIDERACIONES DE SEGURIDAD DE LA INFORMACION

VIDA proporcionará los recursos suficientes para proporcionar una respuesta efectiva de colaboradores y procesos en caso de contingencia o eventos catastróficos que se presenten en la empresa y que afecten la continuidad de su operación.

Además, responderá de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos. VIDA mantendrá canales de comunicación adecuados hacia colaboradores, proveedores y terceras partes interesadas.

19.1.1. Normas de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información

Normas dirigidas a: OFICINA DE RIESGOS

- Debe reconocer las situaciones que serán identificadas como emergencia o desastre para la empresa, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.
- Debe liderar los temas relacionados con la continuidad del negocio y la recuperación ante desastres
- Debe realizar los análisis de impacto al negocio y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.
- Realizado el análisis BIA debe seleccionar las estrategias de recuperación más convenientes para la empresa.
- La Oficina de Riesgos debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.
- Debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

Normas dirigidas a: GERENCIA DE SISTEMAS Y OFICINA DE RIESGOS

- Deben elaborar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.
- Deben participar activamente en las pruebas de recuperación ante desastres y notificar los resultados a la Oficina de Riesgos

Normas dirigidas a: Dirección

- Debe identificar y, al interior de sus áreas, generar la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información. Estos documentos deben ser probados para certificar su efectividad.

19.2. POLÍTICA DE REDUNDANCIA

VIDA propenderá por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la empresa.

19.2.1. Normas de redundancia

Normas dirigidas a: GERENCIA DE SISTEMAS Y OFICINA DE RIESGOS

- Deben analizar y establecer los requerimientos de redundancia para los sistemas de información críticos para la empresa y la plataforma tecnológica que los apoya.

- Debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de VIDA.

- Debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de la empresa.

20. POLÍTICAS DE CUMPLIMIENTO

20.1. POLÍTICA DE CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES

VIDA velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

20.1.1. Normas de cumplimiento con requisitos legales y contractuales

Normas dirigidas a: OFICINA ASESORA JURIDICA Y OFICINA DE RIESGOS

- Deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la empresa y relacionados con seguridad de la información.

Normas dirigidas a: GERENCIA DE SISTEMAS

- Debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo o equipos móviles de la empresa para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.

Normas dirigidas a: TODOS LOS USUARIOS

- No deben instalar software o sistemas de información en sus estaciones de trabajo o equipos móviles suministrados para el desarrollo de sus actividades.

- Deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

20.2. POLÍTICA DE PRIVACIDAD Y PROTECCION DE DATOS PERSONALES

En cumplimiento de la de Ley 18331, por la cual se dictan disposiciones para la protección de datos personales, VIDA a través de la Oficina de Riesgos, propenderá por la protección de los datos personales de sus clientes, proveedores, colaboradores y demás terceros de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para las cuales VIDA, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que en algún momento, por razones de la actividad que desarrolla la empresa, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, VIDA exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales.

Así mismo, buscará proteger la privacidad de la información personal de sus colaboradores, estableciendo los controles necesarios para preservar aquella información que la empresa conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la empresa y no sea publicada, revelada o entregada a colaboradores o terceras partes sin autorización.

20.2.1. Normas de privacidad y protección de datos personales

Normas dirigidas a: AREAS QUE PROCESAN DATOS PERSONALES

- Las áreas que procesan datos personales de beneficiarios, colaboradores, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la empresa.

- Deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.

- Deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.

- Deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.

- Deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

Normas dirigidas a: OFICINA DE RIESGOS

- Debe establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, colaboradores, proveedores y demás terceros de VIDA de los cuales reciba y administre información.

Normas dirigidas a: GERENCIA DE SISTEMAS

- Debe implantar los controles necesarios para proteger la información personal de los beneficiarios, colaboradores, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

Normas dirigidas a: TODOS LOS USUARIOS

- Deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la empresa o de sus colaboradores de cual tengan conocimiento en el ejercicio de sus funciones.

- Es deber de los usuarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

Normas dirigidas a: USUARIOS DE LOS PORTALES DE VIDA

- Deben asumir la responsabilidad individual sobre la clave de acceso a dichos portales que les es suministrada; así mismo, deben cambiar de manera periódica esta clave de acceso.

- Deben contar con controles de seguridad en sus equipos de cómputo o redes privadas para acceder a los portales de VIDA.

- Deben aceptar el suministro de datos personales que pueda hacer la empresa a los terceros delegados para el tratamiento de datos personales, a entidades judiciales y demás entes del Estado que, en ejercicio de sus funciones, solicitan esta información; de igual manera, deben aceptar que pueden ser objeto de procesos de auditoria interna o externa.

20.3 POLÍTICA DE SEGREGACIÓN DE FUNCIONES

Los accesos son aprobados por el Gerente de área respectivo en función de las necesidades. El equipo de infraestructura es el encargado de materializar el acceso.

El control hacia el equipo infraestructura es realizado en forma cruzada dentro del equipo.

21. POLÍTICA DE TELETRABAJO

Normas dirigidas a: TODOS LOS USUARIOS

Se establece la siguiente política de teletrabajo:

- Los accesos deben realizarse únicamente en ambientes seguros y a través de equipos certificados por VIDA
- Accesos a sistemas de propiedad de VIDA solo se realizan a través de conexiones VPN u otras conexiones cifradas. El acceso a VPN esta exclusivamente destinado a ser realizado por computadores certificadas por VIDA
- Los equipos certificados cuentan con autentificación con usuario y clave utilizando remote desktop. Por tanto, las actualizaciones de seguridad instaladas, antivirus y cumplen con las normas de seguridad establecidas están contemplados dentro de la gestión del servidor.
- Aplican las políticas de dispositivos móviles sobre bloqueo remoto que se encuentra en el punto 8 de este manual
- Los horarios de trabajo y tareas a ser realizadas deben ser acordados con el gerente de área responsable.
- Evitar establecer conexiones desde redes no seguras (conexiones Wi-Fi abiertas, redes públicas de hoteles, bibliotecas, centros comerciales, aeropuertos, locutorios, etc.)

.