Manual y Politicas de Seguridad de la Información
PLASPEL SAS
(PR-TIC-01)

VERSIÓN	FECHA	CONTROL DE CAMBIOS	APROBADO
1	23-05-2022	CREACION	GERENTE GENERAL

CONTENIDO

1. INTRODUCCIÓN.

Con la definición de las políticas y estándares de seguridad informática se busca establecer en el interior de PLASPEL SAS una cultura de calidad operando en una forma confiable. La seguridad informática, es un proceso donde se deben evaluar y administrar los riesgos apoyados en políticas y estándares que cubran las necesidades de la Entidad en materia de seguridad.

Las políticas y estándares de seguridad informática establecidas en el presente documento son la base fundamental para la protección de los activos informáticos y de toda la información y Comunicaciones en PLASPEL SAS de manera que esta cumpla con los criterios de Confidencialidad, Integridad y Disponibilidad.

La seguridad de la información es una prioridad para PLASPEL SAS y por tanto es responsabilidad de todos los Colaboradores velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

2. 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 PLASPEL SAS, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

3. DEFINICIONES.

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

- **Acuerdo de Confidencialidad**: es un documento en los que los funcionarios de PLASPEL SAS o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la Entidad, 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.

- **Amenaza**: causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema o a la empresa.

- **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.

- **Comité de Seguridad de la Información**: el Comité de Seguridad de la Información es el órgano que debe establecer los criterios de dirección y control, que permitan implantar los mecanismos más apropiados de protección de la información de PLASPEL SAS, aplicando los principios de confidencialidad, integridad y disponibilidad de la misma y de los recursos informáticos o de otra índole que la soportan, acorde con la planeación estratégica de la empresa.

- **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.

- **Desastre o contingencia**: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras u otros medios necesarios para la operación normal de un negocio.

- **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.

- **Estándar**: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la organización antes de crear nuevas políticas.

- **Estándares de seguridad**: son productos, procedimientos y métricas aprobadas, que definen en detalle como las políticas de seguridad serán implementadas para un ambiente

en particular, teniendo en cuenta las fortalezas y debilidades de las características de seguridad disponibles. Deben estar reflejadas en un documento que describe la implantación de una guía para un componente específico de hardware, software o infraestructura.

- **Evaluación del riesgo**: proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

- **Evento de seguridad de la información**: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

- **Guía**: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares de buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

- **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.

- **Impacto**: la consecuencia que en la empresa se produce al materializarse una amenaza.

- **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 Entidad.

- **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.

- **Mejor Práctica**: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la organización.

- **Organización de seguridad**: es una función que busca definir y establecer un balance entre las responsabilidades y los requerimientos de los roles asociados con la administración de seguridad de la información.

- **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.

- **Políticas**: toda intención y directriz expresada formalmente por el Rol.

- **Procesos**: se define un proceso como cada conjunto de actividades que reciben una o más entradas para crear un producto de valor para el cliente o para la propia empresa (concepto de cliente interno de calidad). Típicamente una actividad empresarial cuenta con múltiples procesos de negocio que sirven para el desarrollo de la actividad en sí misma.

- **Procedimientos**: los procedimientos son los pasos operacionales que los funcionarios deben realizar para alcanzar ciertos objetivos. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una

dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustaran a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

- **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 PLASPEL SAS.

- **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 Entidad. 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.

- **Riesgo**: combinación de la probabilidad de un evento y sus consecuencias.

- **Seguridad de la información**: Preservación de la confidencialidad, integridad y disponibilidad de la información, además involucra otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

- **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 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.

- **Stakeholders:** Para uso práctico del Sistema de Gestión del Riesgo de la Compañía, es toda persona natural o jurídica con la que se tiene relación directa o indirecta (empleados, Consejo de Administración, asociados, proveedores, clientes, pagadurías, bancos y demás).

- **Terceros**: todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

- **TI:** se refiere a tecnologías de la información.

- **TIC:** se refiere a tecnologías de la información y comunicaciones.

- **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 Entidad (amenazas), las cuales se constituyen en fuentes de riesgo.

4. OBJETIVO

Establecer las medidas organizacionales, técnicas, físicas y legales, necesarias para proteger los activos de información contra acceso no autorizado, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir en forma intencional o accidental, en cualquier escenario donde PLASPEL SAS no lo haya autorizado. De esta forma cumplimos en calidad de **buena práctica no obligatoria** con lo requerido en esta materia, concatenado en las normas ISO 27001, Circulares Externas de la Superintendencia Financiera 052 de 2011, 052 de 2007, 042 de 2012; Ley 527-1999 Ley de comercio electrónico, y derivadas de las anteriores

4.1. OBJETIVOS ESPECIFICOS

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de PLASPEL SAS
- Garantizar la continuidad del negocio frente a incidentes.

5. MANUAL DE SEGURIDAD DE LA INFORMACIÓN.

Para PLASPEL SAS la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de las necesidades actuales, PLASPEL SAS implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Los Colaboradores, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de PLASPEL SAS, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

6. COMPROMISO DE LA DIRECCION.

La Gerencia General de PLASPEL SAS aprueba el Manual 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 Alta Dirección de PLASPEL SAS 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 PLASPEL SAS.
- 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. INCUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD.

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 PLASPEL SAS. 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.

8. ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACION.

- PLASPEL SAS 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.

- La Alta Dirección de PLASPEL debe definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.

- La Alta Dirección debe definir y establecer el procedimiento de contacto con las autoridades en caso de ser requerido, así como los responsables para establecer dicho contacto.

- La Alta Dirección debe revisar y aprobar las Políticas de Seguridad de la Información contenidas en este documento.

- La Alta Dirección debe promover activamente una cultura de seguridad de la información en la Entidad.

- La Alta Dirección debe facilitar la divulgación de las Políticas de Seguridad de la Información a todos los funcionarios de la entidad y al personal provisto por terceras partes.

- La Dirección de Tecnología debe asignar las funciones, roles y responsabilidades, a sus funcionarios para la operación y administración de la plataforma tecnológica de PLASPEL SAS. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

- Los Colaboradores y personal provisto por terceras partes que realicen labores en o para PLASPEL SAS, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

9. LÍNEA BASE DE LA POLÍTICA

9.1 RESPONSABILIDAD

Es responsabilidad del Rol de Tecnología hacer uso de la Política de Seguridad de la Información, como parte de sus herramientas de gobierno y de gestión, de definir los estándares, procedimientos y lineamientos que garanticen su cumplimiento y de las demás Áreas, el cumplir lo que a su rol competa en materia de Seguridad de la Información.

9.2 CUMPLIMIENTO

El cumplimiento de la Política de Seguridad de la Información es obligatorio. Si los funcionarios, consultores, contratistas, terceras partes violan estas políticas, la organización se reserva el derecho de tomar las medidas correspondientes.

- PLASPEL SAS ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- PLASPEL SAS protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- PLASPEL SAS protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o

legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- PLASPEL SAS protegerá su información de las amenazas originadas por parte del personal.
- PLASPEL SAS protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- PLASPEL SAS controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- PLASPEL SAS implementará control de acceso a la información, sistemas y recursos de red.
- PALSPEL SAS garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- PLASPEL SAS garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- PLASPEL SAS garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación, basado en el impacto que pueden generar los eventos.
- PLASPEL SAS. garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

9.3 EXCEPCIONES

Las excepciones a cualquier cumplimiento de Política de Seguridad de la Información deben ser aprobadas por el Rol de Tecnología, previo aval de la Gerencia General. Todas las excepciones a la Política deben ser formalmente documentadas, registradas y revisadas.

9.4 ADMINISTRACIÓN DE LAS POLÍTICAS

Las modificaciones o adiciones de la Política de Seguridad de la Información serán propuestas por las Áreas interesada y serán aprobadas por el Gerente General. Estas políticas deben ser revisadas como mínimo una vez al año o cuando sea necesario.

9.4.1. FASES DE IMPLEMENTACIÓN DE LAS POLITICAS DE SEGURIDAD DE INFORMACIÓN

- Desarrollo de las políticas: En esta fase la Entidad debe responsabilizar las áreas para la creación de las políticas, estructurarlas, escribirlas, revisarlas y aprobarlas; por lo cual para llevar a buen término esta fase se requiere que se realicen actividades de verificación e investigación de los siguientes aspectos:
- Justificación de la creación de política: Debe identificarse el por qué la Entidad requiere la creación de la política de seguridad de información y determinar el control al cual hace referencia su implementación.
- Alcance: Debe determinarse el alcance, ¿A qué población, áreas, procesos o departamentos aplica la política?, ¿Quién debe cumplir la política?
- Roles y Responsabilidades: Se debe definir los responsables y los roles para la implementación, aplicación, seguimiento y autorizaciones de la política.
- Revisión de la política: Es la actividad mediante la cual la política una vez haya sido redactada pasa a un procedimiento de evaluación por parte de otros individuos o grupo de individuos que evalúen la aplicabilidad, la redacción y se realizan sugerencias sobre el desarrollo y creación de la misma.
- Aprobación de la Política: Se debe determinar al interior de la entidad la persona o rol de la alta dirección que tiene la competencia de formalizar las políticas de seguridad de la información mediante la firma y publicación de las mismas. Es importante que la Alta Gerencia de la Entidad muestre interés y apoyo en la implementación de dichas políticas.
- Cumplimiento: Fase mediante la cual todas aquellas políticas escritas deben estar implementadas y relacionadas a los controles de seguridad de la Información, esto con el fin de que exista consistencia entre lo escrito en las políticas contra los controles de seguridad implementados y documentados.
- Comunicación: Fase mediante la cual se da a conocer las políticas a los funcionarios, contratistas y/o terceros de la Entidad. Esta fase es muy importante toda vez que del conocimiento del contenido de las políticas depende gran parte del cumplimiento de las mismas; esta fase de la implementación también permitirá obtener retroalimentación de la efectividad de las políticas, permitiendo así realizar excepciones, correcciones y ajustes pertinentes. Todos los funcionarios contratistas y/o terceros de la entidad debe conocer la existencia de las políticas, la obligatoriedad de su cumplimiento y la ubicación física de tal documento o documentos, para que sean consultados en el momento que se requieran.
- Monitoreo: Es importante que las políticas sean monitoreadas para determinar la efectividad y cumplimiento de las mismas, deben crearse mecanismos ejemplo indicadores para verificar de forma periódica y con evidencias que la política funciona y si debe o no ajustarse.
- Mantenimiento: Esta fase es la encargada de asegurar que la política se encuentra actualizada, integra y que contiene los ajustes necesarios y obtenidos de las retroalimentaciones.

- Retiro: Fase mediante la cual se hace eliminación de una política de seguridad en cuanto esta ha cumplido su finalidad o la política ya no es necesaria en la Entidad. Esta es la última fase para completar el ciclo de vida de las políticas de seguridad y requiere que este retiro sea documentado con el objetivo de tener referencias y antecedentes sobre el tema.

9.4.2. DESCRIPCIÓN DE LAS POLÍTICAS Y ESTÁNDARES

La información es un activo que la compañía considera esencial para las actividades de la empresa y debe ser protegida de acuerdo con los principios de confidencialidad, integridad y disponibilidad. A través de esta Política se difunden los objetivos de seguridad de la información de la compañía, que se consiguen a través de la aplicación de controles de seguridad, para gestionar un nivel de riesgo aceptable. Este documento tiene el objetivo de garantizar la continuidad de los servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los objetivos de negocio y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad

10. POLÍTICAS GENERALES.

10.1. Responsabilidad sobre los activos y recursos informáticos.

PLASPEL SAS pone al servicio de los funcionarios el uso de los medios necesarios para el normal desarrollo de las labores propias de sus respectivos cargos, para lo cual adopta y comunica las políticas de uso aceptable, controles y medidas dirigidas a garantizar la seguridad y continuidad del servicio que presta.

10.2. Uso aceptable de los activos y recursos informáticos.

Todos los colaboradores, consultores, contratistas, terceras partes, que usen activos de información que sean propiedad de PLASPEL SAS, son responsables de cumplir y acoger con integridad la política de uso aceptable para dar un uso racional y eficiente los recursos asignados.

10.3. Usuarios informáticos.

La jefatura de Gestión Humana debe notificar al Rol de Tecnología todas las novedades del personal directo e indirecto que sean usuarios de activos y recursos informáticos tales como ingresos, traslados, licencias, retiros y vacaciones.

10.3.1. Usuarios Nuevos.

Todo el personal nuevo de PLASPEL SAS, deberá ser comunicado por el Rol de Tecnología, para asignarle los derechos correspondientes como usuario informático (Equipo de Cómputo, Creación de Usuario para la Red, Perfil de usuario en el Directorio Activo) y cuenta de correo corporativo.

10.3.2. Retiro parcial del usuario.

Cuando el usuario informático de ausenta de sus labores por causa de vacaciones, incapacidades o licencias debe ser informada esta situación por el Jefe inmediato al Rol de tecnología para inactivar parcialmente los derechos del usuario informático.

10.3.3. Retiro definitivo del usuario.

En caso de retiro definitivo del Colaboradores en PLASPEL SAS, el Rol de Tecnología anulará y cancelará todos los derechos otorgados como usuario informático.

10.3.4. Obligaciones de los Usuarios.

- Todos los usuarios de servicios de información son responsables por el de usuario y contraseña que recibe para el uso y acceso de los recursos.

- Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por el Rol de Tecnología antes de poder usar la infraestructura tecnológica en PLASPEL SAS.

- Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de PLASPEL SAS, a menos que se tenga el visto bueno de la Gerencia General.

- Cada usuario que acceda a la infraestructura tecnológica de PLASPEL SAS debe contar con un identificador de usuario (ID) único y personalizado. Por lo cual no está permitido el uso de un mismo ID por varios usuarios.

- Los funcionarios son responsables de todas las actividades realizadas con su identificador de usuario (ID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el ID de otros usuarios.

- Los usuarios deberán mantener sus equipos de cómputo bloqueados cuando no se encuentren en su lugar de trabajo.

10.3.5. Derechos de usuarios.

Capacitación en seguridad informática: Todo empleado en PLASPEL SAS deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática, donde se den a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento.

10.3.6. Sanciones a usuarios.

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de PLASPEL SAS, o de que se le declare culpable de un delito informático.

10.4. Controles de acceso físico.

- El ingreso y salida de los visitantes a las áreas de trabajo en PLASPEL SAS deben ser registrados en la recepción, indicado la fecha y hora de entrada y salida de los mismos.

- Cualquier persona que tenga acceso a las instalaciones de PLASPEL SAS y que ingresa con equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la entidad, deben ser registrados al momento de su entrada, en el Rol de recepción o portería, el cual podrán retirar el mismo día. En caso

contrario deberá tramitar ante el Rol de Tecnología la autorización de salida correspondiente.

- El cuarto de Servidores es un Rol restringida, por lo que solo el personal del Rol de Tecnología puede acceder a él.

10.5. Seguridad física y del Medio Ambiente.

- El usuario o funcionario deberá reportar de forma inmediata al Rol de Tecnología cuando se detecte riesgo real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.

- El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.

- Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

10.6. Protección y ubicación de los equipos.

- Los funcionarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del Rol de Tecnología, en caso de requerir este servicio deberá solicitarlo.

- El Rol de Tecnología será la encargada de generar el resguardo y recabar la firma del funcionario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por Tecnología.

- El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de los empleados de PLASPEL SAS.

- Será responsabilidad del funcionario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

- Es responsabilidad de los funcionarios almacenar su información únicamente en la partición del disco duro diferente destinada para archivos de programas y sistemas operativos: Documentos / Mis documentos

- Se debe evitar colocar objetos encima del equipo de cómputo o tapar las salidas de ventilación del monitor o de la CPU.

- El funcionario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar un reubicación de cables con el personal de Tecnología.

- Queda prohibido que el funcionario distinto al personal de Tecnología abra o destape los equipos de cómputo.

10.6. Mantenimiento de equipos.

- Únicamente el personal autorizado por el Rol de Tecnología podrá llevar a cabo los servicios y reparaciones al equipo informático.

- Los funcionarios deberán asegurarse de almacenar la información en la carpeta de BACKUP creada en cada equipo de cómputo con el fin de respaldar la información generada con copias de seguridad programados a esta carpeta la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

10.7. Uso de dispositivos extraíbles.

- El acceso a los dispositivos de almacenamiento externo como Memorias USB, Discos portátiles, Unidades de Cd y DVD Externos, está restringido en PLASPEL SAS.

- Si algún Rol o dependencia por requerimientos muy específicos del tipo de aplicación o servicios de información tengan la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por el Rol de Tecnología con el respectivo visto del Jefe de la Dependencia.

- El funcionario que se les permita el uso de estos dispositivos será responsable del buen uso de ellos.

10.8. Administración de operaciones en los equipos de cómputo.

- Los Colaboradores deberán proteger la información utilizada en la infraestructura tecnológica de PLASPEL SAS. De igual forma la información reservada o confidencial que deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna de la empresa a otras dependencias y/o regionales o redes externas como internet.

- Los usuarios y Colaboradores de PLASPEL SAS que hagan uso de equipos de cómputos, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red.

- Cuando un funcionario no autorizado o un visitante requieran la necesidad de ingresar al cuarto de Servidores, debe solicitar mediante comunicado interno debidamente firmado y autorizado por el Director de Tecnología y para un visitante se debe solicitar la visita con anticipación, y donde se especifique tipo de actividad a realizar, y siempre contar con la presencia de un funcionario del Rol de Tecnología.

- El equipo de cómputo, periférico o accesorio de tecnología de información que sufra algún desperfecto, daño por maltrato, descuido o negligencia por parte del usuario responsable, se levantara un reporte de incumplimiento de políticas de seguridad.

- El técnico de soporte del Rol de tecnología asegura mediante el instructivo de Borrado seguro la eliminación de la información de los equipos de cómputo que deban ser reasignados a nuevos funcionarios.

- El técnico de soporte del Rol de tecnología asegura con la aplicación del instructivo de borrado seguro que los equipos de cómputo que sufran daños irreparables y deban ser dados de baja del inventario de activos en PLASPEL SAS deberán aplicarse las actividades y

los controles necesarios para el formateo y destrucción de los mismos con el fin de asegurar que su eliminación se realiza de forma segura.

10.4. Política de escritorio y pantalla limpia.

Con el fin de reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios, se deben tener en cuenta las siguientes pautas:

- El personal de PLASPEL SAS debe conservar su escritorio libre de información propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

- El personal de PLASPEL SAS debe bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.

- Al imprimir documentos de carácter confidencial, estos deben ser retirados de la impresora inmediatamente.

10.5. Uso de impresoras y del servicio de Impresión.

Asegurar la operación correcta y segura de las impresoras y del servicio de impresión, siguiendo los siguientes lineamientos:

- Los documentos que se impriman en las impresoras del PLASPEL SAS deben ser de carácter institucional.

- Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.

- Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar al Rol de Tecnología.

10.9. Uso del Correo electrónico.

El uso de Internet debe estar destinado exclusivamente a la ejecución de las actividades de la organización y deben ser utilizados por el empleado para realizar las funciones establecidas para su cargo, por lo cual se definen los siguientes parámetros para su uso:

- El Rol de Tecnología será la encargada de proporcionar el servicio de correo corporativo, así como vigilar su correcto uso y funcionamiento. Para tal fin asignará una cuenta que tiene asociado un buzón de correo, en el cual se almacenan todos los mensajes enviados y recibidos.

- Cada usuario debe depurar continuamente su buzón de correo con el fin de mantener siempre espacio disponible para nuevos mensajes.

- La información contenida en el correo se considera información privada y por lo tanto debe ser manejada como una comunicación privada y directa entre el remitente y su destinatario.

- La cuenta de correo es intransferible y no se puede compartir la cuenta.

- Cada usuario es responsable de la información enviada o reenviada desde su cuenta de correo.

- Aunque la entidad cuenta con un servicio de revisión de virus para los mensajes de correo electrónico entrante, los usuarios del correo deben ser cuidadosos cuando decidan abrir los archivos anexos colocados en mensajes de remitentes desconocidos o sospechosos. Si llegan mensajes con esta característica, se debe informar al Rol de Tecnología.

- Los empleados de PLASPEL SAS no pueden emplear direcciones de correo electrónico diferentes a las cuentas oficiales para atender asuntos de la Entidad.

- Los usuarios del correo corporativo no deben enviar correos con documentos adjuntos donde su peso sea superior a 8 Megas.

- Está prohibido enviar o contestar cadenas de mensajes a una persona o grupo de personas.

- Los usuarios del correo corporativo no deben promocionar a través de la cuenta corporativa bienes o servicios particulares que no tengan relación con los objetivos de PLASPEL SAS.

- Es prohibido utilizar el correo electrónico para fines diferentes a los objetivos de PLASPEL SAS.

- Los usuarios del correo corporativo no deben falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

- Es prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

10.10. Controles contra virus o software malicioso.

- La Dirección de Tecnología debe proveer que en todos los equipos de cómputo este instalado el software antivirus y su actualización mediante una tarea programada.

- Para prevenir infecciones por virus informático, los usuarios de los equipos de cómputo en PLASPEL SAS no deben hacer uso de software que no haya sido proporcionado y validado por el Rol de Tecnología.

- Todos los archivos de equipos que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.

- Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y notificar al Rol de Tecnología para la revisión y erradicación del virus.

10.11. Recursos compartidos.

El uso de carpetas compartidas en la red de PLASPEL SAS es una práctica que, aunque puede ser una herramienta útil de trabajo, tiene implícitos algunos riesgos que pueden afectar los

principios de confidencialidad, integridad y disponibilidad de la información, por lo tanto su uso y aplicación es controlado.

Con este propósito se definen los siguientes lineamientos para su uso seguro:

- El técnico de soporte establece e implementa, en los casos aprobados, la configuración de acceso a la carpeta, previo requerimiento formal de la misma a través del Rol de tecnología.

- Los usuarios a quienes se les autoriza y dispone el recurso compartido son los responsables por las acciones y los accesos sobre la información contenida en dicha carpeta.

10.12. Controles para la Generación y Restauración de Copias de Respaldo (Backups).

Procedimiento de generación y restauración de copias de respaldo para salvaguardar la información crítica de los procesos significativos de la entidad. Se consideran como mínimo los siguientes aspectos:

- La dirección de tecnología efectuará mediante tarea programada la copia de seguridad a la carpeta de BACKUP creada en cada equipo de cómputo.

- El almacenamiento de la información en esta carpeta es responsabilidad de cada usuario.

- Se efectuará copia de seguridad a la información de las carpetas compartidas y con acceso restringido a usuarios autorizados.

- Las copias de seguridad se efectuarán semanalmente los días viernes a las 17:30 horas.

10.13. Navegación en Internet.

El acceso a Internet provisto a los usuarios y funcionarios de PLASPEL SAS es exclusivamente para las actividades relacionadas con las necesidades del cargo y funciones desempeñadas.

Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que:

- Serán sujetos de monitoreo de las actividades que realiza en internet, saben que existe la prohibición al acceso de páginas no autorizadas, saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.

- Saben que existe la prohibición de descarga de software sin la autorización del Rol de Tecnología.

- La utilización de Internet es para el desempeño de sus funciones y cargo en PLASPEL SAS y no para propósitos personales.

- La Dirección de Tecnología a través de herramientas de monitoreo y análisis de tráfico, detectará a los usuarios que hagan mal uso de los servicios de Internet.

- El Rol de Tecnología, se encuentra facultada para bloquear todos aquellos sitios de Internet que considere que no son compatibles con las labores de los funcionarios. En caso de existir excepciones por causas debidamente justificadas, el Jefe de la Dependencia correspondiente deberá presentar la solicitud mediante memorando, exponiendo las causas de la excepción ante el Rol de Tecnología para su estudio y aprobación.

- Se permitirá el acceso al Wi-Fi a los visitantes y proveedores que lo requieran, previa solicitud al Rol de Tecnología del funcionario encargado del personal visitante.

- Se prohíbe el ingresar a páginas pornográficas, descargar de música y video, en especial con los servicios provistos por las páginas especializadas para tal fin, así como utilizar o participar en juegos de entretenimiento en línea.

- No utilizar los servicios de radio y TV a través de Internet, en caso de requerirse esta información para el desarrollo de las funciones a su cargo, el Jefe de la Dependencia correspondiente deberá presentar la solicitud mediante memorando, exponiendo las causas de la excepción ante el Rol de Tecnología para su estudio y aprobación.

- No ingresar a páginas relacionados con redes sociales durante la jornada laboral.

- La descarga de archivos de internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio de Internet, en forma específica el usuario debe cumplir los requerimientos de la política de uso de internet descrita en este manual.

10.14. Controles para Otorgar, Modificar y Retirar Accesos a Usuarios.

- La creación de un nuevo usuario dentro de los sistemas de Información en PLASPEL SAS, deberá ser enviada al Rol de Tecnología acompañada de la solicitud debidamente firmada por el Jefe de Área, de lo contrario no se le dará trámite a dicha requisición.

- El Rol de Tecnología, en cabeza del director de Tecnología, será responsable de ejecutar los movimientos de altas, bajas o cambios de perfil de los usuarios.

- La creación de tarjetas de ingreso de nuevos usuarios para sede principal de PLASPEL SAS debe ser enviada al director de Tecnología por el Jefe de Recursos Humanos con los datos del usuario a crear y los privilegios de acceso que debe tener.

10.15. Administración y uso de contraseñas.

- La asignación de contraseñas es realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.

- Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá acudir al Rol de Tecnología para que se le proporcione una nueva contraseña.

- Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.

- Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con el mismo.

- Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, deberá cambiarla inmediatamente.

10.16. Adquisición de Software.

- Se considera una falta grave el que los funcionarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de PLASPEL SAS, que no esté autorizado por el Rol de Tecnología.

- El control de manejo para las licencias y el inventario de los Medios, será responsabilidad del Rol de Tecnología.

- El Rol de Tecnología debe mantener un inventario de equipos físicos y de los programas instalados y pueden borrar o instalar programas o software autorizados y legalmente licenciados.

10.17. Cumplimiento de Seguridad Informática Política.

El Rol de Tecnología tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

Derechos de propiedad intelectual, los sistemas desarrollados por personal interno o externo que controle el Rol de Tecnología son propiedad intelectual de PLASPEL SAS.

10.18. Cláusulas de cumplimiento.

- El Rol de Tecnología realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática.

- El Rol de Tecnología podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado a la Gerencia General.

- Los jefes y responsables de los procesos establecidos en PLASPEL SAS deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y estándares de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

10.19. Violaciones de seguridad Informática.

- Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática.

- Ningún funcionario de PLASPEL SAS debe probar o intentar probar fallas de la Seguridad Informática conocidas.

- No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información de PLASPEL SAS.

11.1. ORGANIZACIÓN DE SEGURIDAD

11.1.1. Política de la organización de seguridad

El Rol de Tecnología es responsable de definir, coordinar y controlar la gestión necesaria para mitigar los riesgos asociados a la seguridad de la información en PLASPEL SAS y reportará al COMITÉ DE SEGURIDAD DE LA INFORMACIÓN, dicho comité está constituido por el Rol de Tecnología, que preside; el Rol de Riesgos y los roles que eventualmente sean requeridos, con el objeto de cumplir y soportar las actividades de Seguridad de la Información.

11.2.1. Estándares de la Política de la organización de seguridad

11.2.1.2. Responsabilidades para la seguridad de la información.

PLASPEL SAS es el propietario de la información. Su tenencia y manejo es delegada a los responsables de las Áreas, quienes son responsables de la custodia de la información que generan y usan, considerando su propósito y uso. Por ello los responsables de Rol deben ser conscientes de los riesgos a la que está expuesta la información a su cargo, de forma que ejerzan frente a sus funcionarios el liderazgo apropiado para disminuirlos.

11.2.2. Contacto con autoridades y grupos de interés.

PLASPEL SAS, debe mantener contacto con las autoridades y grupos de interés para estar al corriente en cambios de normativa del gobierno electrónico en Colombia e identificar las tendencias en Seguridad de la Información.

11.2.3. Revisión independiente en seguridad de la información.

Auditoría Interna debe implementar y ejecutar un plan interno de auditoría de seguridad de la información. Este plan debe estar enfocado hacia la revisión de todos los requerimientos (políticas y procedimientos) de seguridad. Los resultados deben generar un programa de seguridad, que incluya como mínimo: acciones a realizar, tablas de tiempo y responsables. El programa debe ser aprobado por el Comité de Seguridad de la Información.

11.2.4. Seguridad en los Accesos por Terceros.

El Rol de Tecnología debe realizar una evaluación de riesgos para identificar el riesgo de acceso por terceros a la información de PLASPE SAS. Cada Rol debe verificar la implementación de acuerdos, monitorear el cumplimiento de ellos y gestionar los cambios para asegurar que los servicios que se prestan cumplen los requisitos acordados con los terceros.

Todo requerimiento de acceso o utilización del componente Tecnológico de PLASPEL SAS por parte de un tercero requiere la realización de un análisis de riesgos previo a la utilización de dichos recursos. Este análisis debe ser efectuado por el Comité de Seguridad de la Información en conjunto con el administrador de la plataforma Tecnológica.

El análisis de riesgos se debe efectuar a cualquier tercero que requiera tener interacción con los componentes tecnológicos, sistemas de información y redes de datos de PLASPEL SAS.

La identificación y análisis de los riesgos debe realizarse teniendo en cuenta los siguientes aspectos:

- El tipo de servicio y el acceso físico y lógico a utilizar.
- El tipo de información y su criticidad.
- El personal del tercero que va a interactuar.
- El nivel de impacto que tendrá el acceso a los recursos por parte del tercero.
- Los requerimientos legales y regulatorios relevantes asociados con el tercero y con las actividades a desarrollar.

En el caso de presentarse un contrato con un tercero (clientes o proveedores), las políticas de Seguridad de la Información aplican de igual forma a los terceros, así mismo deben cumplir las leyes y regulaciones nacionales e internacionales respecto a derechos de autor y

propiedad intelectual, comercio electrónico e intercambio electrónico de datos. Cualquier falta a las políticas de seguridad de la información, por parte de un externo, estará sujeta a las medidas establecidas por PLASPEL SAS. Todo cambio a nivel tecnológico debe ser informado previamente a PLASPEL SAS y autorizado por la Compañía.

En las relaciones con los clientes, el tercero es quien define los parámetros iniciales de seguridad de la Información de acuerdo con sus políticas internas y es deber de la Gerencia de Tecnología Informática

11.3. CLASIFICACIÓN Y CONTROL DE ACTIVOS DE INFORMACIÓN

11.3.1. Política para la clasificación y control de activos de información

La información debe estar inventariada y tener identificados los riesgos y exposiciones de seguridad; con el objetivo de evitar pérdidas financieras, operativas y/o de imagen para la compañía, la información deberá estar clasificada como secreta, restringida o general. La información secreta y restringida debe estar soportada por un acuerdo de confidencialidad o de no-divulgación cuando sea compartida con terceros.

11.3.2. Estándares de la Política de clasificación y control de activos de información

11.3.2.1. Responsabilidad sobre los activos.

PLASPEL SAS pone al servicio de los funcionarios el uso de los medios necesarios para el normal desarrollo de las labores propias de sus respectivos cargos, para lo cual adopta y comunica las políticas de uso aceptable, controles y medidas dirigidas a garantizar la seguridad y continuidad del servicio que presta.

Respecto a los propietarios de los activos de información, los usuarios de información deben actuar como propietarias de la información física y electrónica de la entidad, 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 la validez de los usuarios y sus perfiles de acceso a la información. Deben ser conscientes que los recursos de procesamiento de información del instituto, se encuentran sujetos a auditorías y a revisiones de cumplimiento por parte de los entes de control.

11.3.2.2. Metodología de clasificación de activos.

Para asegurar que los activos de información reciben el nivel de protección adecuado, el Rol de Tecnología es responsable de definir la metodología de clasificación de activos de información, estos se deben clasificar según la necesidad, las prioridades y el grado de protección esperado en el manejo de los mismos.

11.4 USO ACEPTABLE DE LOS ACTIVOS Y RECURSOS

11.4.1. Política de Uso Aceptable de los Activos y Recursos de información

Todos los funcionarios, consultores, contratistas, terceras partes, que usen activos de información que sean propiedad de PLASPEL SAS, son responsables de cumplir y acoger con integridad la Política de Uso Aceptable para dar un uso racional y eficiente los recursos asignados. Estándares para el uso aceptable de los activos de información Política Seguridad de la información

11.4.2. Uso de los sistemas y equipos de cómputo.

La organización tiene regla de renuncia (disclaimer) que debe utilizarse al inicio de sesión en los equipos de cómputo:

"¡*Advertencia! Este sistema (hardware, software y periféricos), así como la información en él contenida es propiedad de la empresa y su uso está restringido únicamente para propósitos de su negocio, reservándose el derecho de monitorearlo en cualquier momento. Cualquier utilización, modificación o acceso no autorizado a este sistema dará lugar a las acciones disciplinarias y/o legales que correspondan. El ingreso y utilización de este sistema implica su consentimiento con esta política*."

El Rol de Tecnología 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 PLASPEL SAS Debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica. 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 funcionarios del instituto 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 del instituto 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 el Rol de Tesorería para proteger su acceso de los demás funcionarios de la red de la empresa. Debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios del instituto, ya sea cuando son dados de baja o cambian de usuario. Debe revisar los accesos físicos en horas no hábiles a las áreas donde se procesa información.

El Rol de Auditoria Interna 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.

El Rol de Riesgos debe evaluar y analizar los informes de verificación de equipos de cómputo de las diferentes áreas del instituto, en particular de las áreas sensibles.

11.4.3. Correo electrónico.

La organización, como muestra del respeto por los principios de libertad de expresión y privacidad de información, no genera a los funcionarios ninguna expectativa de privacidad en cualquier elemento que almacene, envíe o que reciba por medio del sistema de correo electrónico propiedad de la compañía; en consecuencia, podrá denegar el acceso a los servicios de correo electrónico, inspeccionar, monitorear y/o cancelar un buzón de correo asignado. Las comunicaciones por correo electrónico entre la empresa y sus públicos de interés deben hacerse a través del correo homologado y proporcionado por la empresa. No es permitido utilizar cuentas personales para comunicarse con los públicos de interés de la organización, ni para transmitir cualquier otro tipo de información del negocio. A los funcionarios que de acuerdo con sus funciones requieran una cuenta de correo, esta se les asigna una vez son vinculados. El Rol de Gestión Humana es responsable de informar al Rol de Tecnología, las vinculaciones que requieran creación de cuenta de correo; de igual manera debe informar oportunamente los retiros de funcionarios para la suspensión de este servicio. Esta cuenta estará activa durante el tiempo que dure la vinculación del colaborador con la compañía, excepto en casos de fuerza mayor o mala utilización que eventualmente

puedan causar la suspensión o cancelación de la misma. Una vez se produzca la desvinculación de la persona, la cuenta será dada de baja en el servidor mediante una solicitud enviada a la mesa de servicios. La capacidad máxima para almacenamiento de correo electrónico está definida por el Rol de Tecnología y depende del tipo de usuario. No obstante, en caso de necesidades especiales, el interesado podrá solicitar la ampliación de la capacidad. De igual manera, en caso de necesidad (por razones del negocio o técnicas), las capacidades máximas de los buzones podrán ser modificadas unilateralmente por parte de la compañía.

El sistema de monitoreo filtrará los archivos anexos a los mensajes de correo electrónico, para verificar la ausencia de virus. La entrega de todo mensaje a su destinatario final está sujeta a que esta comprobación sea exitosa. La organización tiene regla de renuncia (disclaimer) que debe utilizarse siempre en los mensajes. Para evitar reclamaciones legales todos los usuarios de correo de la empresa tienen que hacer pública la renuncia de responsabilidad legal por el envío de la información. El disclaimer aprobado es:

"La información contenida en este mensaje y en sus anexos es estrictamente confidencial. Si usted recibió por error esta comunicación, por favor notificar inmediatamente esta circunstancia mediante reenvío al mail del remitente y bórrela puesto que su uso no autorizado acarreará las sanciones y medidas legales a que haya lugar. La empresa no se hace responsable por la presencia en este mensaje o en sus anexos, de algún virus o malware que pueda generar o genere daños en sus equipos, programas o afecte su información.

The information contained in this message and its attachments is strictly confidential. If you received this communication in error, please immediately notify the sender of the situation by replying it to sender email address and delete this message as its unauthorized use shall derive in applicable penalties and legal actions.. The Company is not liable for the presence of any virus or malware in this message or its attachments that cause or may cause damage to your equipment, software or that affects your information."

El buzón de correo es personal e intransferible y corresponde al colaborador velar por la seguridad protegiendo su clave de acceso. El usuario es el único responsable por el buen uso de su cuenta de correo electrónico. En consecuencia, al aceptar el buzón otorgado por la organización, el usuario se compromete a:

- Respetar la privacidad de las cuentas de otros usuarios del servicio, tanto dentro como fuera de la red corporativa. El usuario no podrá utilizar identidades ficticias o pertenecientes a otros usuarios para el envío de mensajes.
- El colaborador titular de correo o cuenta asignada por la organización, usará el correo electrónico para enviar y recibir mensajes necesarios para el desarrollo de las labores

propias de su cargo o de las investigaciones que tenga asignadas; solo personas responsables de Rol pueden aprobar envíos masivos de correos a los funcionarios de la empresa.

- El uso del correo electrónico propiedad de la compañía deberá ser usado solamente para fines propios a la organización. En su uso el colaborador actuará siempre con respeto y cortesía; no podrá crear, distribuir o reenviar mensajes que ofendan la dignidad, intimidad y buen nombre de las personas, de las instituciones, o para realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil; de igual forma se prohíbe difundir ideas políticas, religiosas, propagandas entre otros.
- La compañía se abstiene de enviar o recibir los mensajes de sus usuarios con contenido impropio, difamatorio, ilícito, obsceno, indecente o que contengan difusión de noticias sin identificar plenamente su autor; adicionalmente, los funcionarios no podrán enviar anónimos, propagandas o literatura de cualquier índole, encuestas, concursos, esquemas piramidales, cartas en cadena, mensajes no deseados, o cualesquiera que contenga mensajes duplicativos o no solicitados, u otra información ajena a las labores que desempeñan en su cargo.
- Los funcionarios de la compañía se abstendrán de utilizar la cuenta para el envío o reenvío de mensajes spam (no solicitados, no deseados o de remitente desconocido, habitualmente de tipo publicitario, enviados en grandes cantidades), hoax (es un intento de hacer creer que algo falso es real), con contenido que pueda resultar ofensivo o dañino para otros usuarios (como virus o pornografía), o que sea contrario a las políticas y normas institucionales.
- Evitar el envío desde su buzón de elementos (textos, software, música, imágenes o cualquier otro) que contravengan lo dispuesto en la legislación vigente y en los reglamentos internos, sobre propiedad intelectual y derechos de autor. En especial, es necesario evitar la distribución de software que requiera licencia, claves ilegales de software, programas para romper licencias (crackers), y en general, cualquier elemento u objeto de datos sin permiso específico del autor cuando este sea requerido. La violación de esta obligación origina automáticamente la suspensión del servicio y puede ser causa de sanciones al usuario, con perjuicio de las responsabilidades que eventualmente puedan surgir ante la ley.
- Realizar mantenimiento periódico de su correo, cuando el sistema le haga advertencias de espacio disponible. Estas advertencias se realizan varias veces, por lo que debe estar atento e informar a la mesa de servicios informáticos, cuando requiera la depuración del mismo.
- Utilizar la cuenta de correo electrónico corporativa para fines laborales, de investigación y los estrictamente relacionados con las actividades propias de su trabajo. Los

funcionarios deben evitar usar el buzón de correo electrónico para fines comerciales diferentes a los que sean relativos al interés de la empresa.

- El colaborador debe depurar mensualmente el contenido del buzón de entrada en el servidor para evitar que los mensajes permanezcan en él un tiempo excesivo que conduzca a la congestión o al bloqueo del mismo.
- Respetar la privacidad de las cuentas de otros usuarios del servicio, tanto dentro como fuera de la red corporativa.
- Evitar el envío de respuestas con copia a todos los destinatarios de un mensaje recibido, y en particular cuando se trata de mensajes que originalmente hayan sido dirigidos a un grupo grande de usuarios; salvo cuando se trate de una respuesta que por su naturaleza o contenido necesariamente requiera ser conocida por todos ellos.
- Evitar abrir mensajes no esperados que contengan archivos adjuntos, aunque provengan de personas conocidas. Podría tratarse de un virus. En particular, no abrir mensajes cuyo asunto contenga palabras en inglés a menos que lo esté esperando.
- En lo posible, es necesario evitar usar letras mayúsculas, especialmente en el campo de "Asunto:", al igual que el uso excesivo de signos de exclamación (&, %, $, #, ?, i, !, ¿), esto puede hacer que los sistemas de correo lo identifiquen como correo no deseado, y el mensaje posiblemente no llegue al destinatario, o llegue con identificación de correo no solicitado.
- Si utiliza el servicio de correo a través del sitio web de la empresa, se recomienda que no deje mensajes almacenados por mucho tiempo en el servidor de correo. Tenga presente descargarlos con frecuencia, preferiblemente a diario. Tenga en cuenta que el tamaño de su buzón de correo es limitado; una vez superado este tope, el sistema no procesará más correos. Elimine mensajes si lo necesita y vacíe la papelera siempre que sea posible.

11.4.5. Uso de herramientas que comprometen la seguridad.

Hacer o intentar hacer, sin permiso del dueño o del anfitrión del sistema o del Rol de Tecnología, cualquiera de los siguientes actos:

- Acceder el sistema o red.
- Monitorear datos o tráfico.
- Sondear, copiar, probar firewalls o herramientas de hacking.
- Atentar contra la vulnerabilidad del sistema o redes.
- Violar las medidas de seguridad o las rutinas de autenticación del sistema o de la red.

11.4.5.1. Recursos compartidos.

El uso de carpetas compartidas en los equipos de cómputo de los usuarios es una práctica que, aunque puede ser una herramienta útil de trabajo, tiene implícitos algunos riesgos que pueden afectar los principios de confidencialidad, integridad y disponibilidad de la información, por lo tanto su uso y aplicación debe ser controlado. Con este propósito la organización define los siguientes lineamientos para su uso seguro:

- Se debe evitar el uso de carpetas compartidas en equipos de escritorio.
- Los administradores de la red establecen e implementan, en los casos aprobados, la configuración de acceso a la carpeta, previo requerimiento formal de la misma a través de la Mesa de Servicios.
- El usuario que autoriza y dispone el recurso compartido es el responsable por las acciones y los accesos sobre la información contenida en dicha carpeta.
- Se debe definir el tipo de acceso y los roles estrictamente necesarios sobre la carpeta (lectura, escritura, modificación y borrado).
- Debe tenerse claramente especificado el límite de tiempo durante el cual estará publicada la información y compartido el recurso en el equipo.
- Si se trata de información confidencial o crítica para la empresa, deben utilizarse las carpetas destinadas para tal fin en el servidor de archivos de usuarios, para que sean incluidos en las copias diarias de respaldo de información o implementar herramientas para el respaldo continuo de información sobre dichos equipos.
- El acceso a carpetas compartidas debe delimitarse a los usuarios que las necesitan y deben ser protegidas con contraseñas.
- No se debe permitir el acceso a dichas carpetas a usuarios que no cuenten con antivirus corporativo actualizado.

11.4.5.2. Sitios Web para compartir documentos.

El dueño del sitio será el responsable de la seguridad del mismo y del acceso a la información que se encuentra alojada.

- El dueño del sitio será el responsable de otorgar los permisos requeridos.
- El dueño del sitio definirá un delegado que tengan control total sobre el sitio, a manera de contingencia, para la asignación de los permisos requeridos en su ausencia.

11.4.5.3. Computación en nube.

Ninguna información de PLASPEL SAS podrá utilizar tecnologías de computación en nube si no está previamente autorizado por el Rol de Tecnología.

11.4.5. Uso equipos portátiles y dispositivos móviles.

Los funcionarios, contratistas y terceros se comprometen a hacer uso adecuado de los dispositivos móviles para el acceso a los servicios corporativos de movilidad proporcionados por la empresa, tales como escritorios y aplicaciones virtuales, correo, comunicaciones unificadas, redes virtuales privadas (VPN), entre otros, atendiendo las siguientes directrices:

- El dispositivo móvil debe estar en el bolsillo, maletín o lugar no visible en partes públicas.
- El dispositivo móvil debe estar configurado para bloqueo automático por un tiempo de inactividad a través de medios disponibles de configuración tales como contraseña, patrón huella dactilar, reconocimiento de voz, entre otras.
- Uso de aplicación de antivirus.
- Uso de canales seguros y cifrados cuando se conecte a redes compartidas de acceso libre, no seguras.

11.4.5. Acceso de equipos distintos a los asignados.

Todos los funcionarios de la Compañía, desde su rol y competencia, tiene la obligación de:

- Desactivar la opción de autoguardado de contraseñas en los diferentes navegadores web.
- No dejar claves en ningún sistema de almacenamiento de información web.
- Creación de contraseñas seguras, no incluir información personal como nombres, fechas de nacimiento, otros.
- Cerrado de sesión de escritorio virtual cuando no esté en uso.

El Rol de Tecnología debe implementar las medidas necesarias para protección frente al riesgo de la utilización de equipos y comunicación móvil. Se prestará especial cuidado para asegurar que no se compromete la información del negocio, teniendo en cuenta los riesgos que conlleva el trabajar con el equipo móvil en entornos desprotegidos. La utilización de los servicios móviles conectados a las redes, debe tener una protección idónea. El acceso remoto a la información del negocio a través de redes públicas usando servicios de computación móvil, sólo debería tener lugar después de la identificación y autenticación exitosa y con el establecimiento de los mecanismos adecuados del control del acceso.

11.5. TRATAMIENTO Y GESTIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN

11.5.5. Política del Tratamiento y Gestión del Riesgo en Seguridad de la Información

El Rol de Tecnología, es responsable de analizar los riesgos en seguridad de la información, con base en los objetivos de negocio y de acuerdo con la Política de Gestión de Riesgos y con aprobación del Comité de Seguridad de la Información. Los responsables de Áreas son responsables de priorizar y realizar el tratamiento de los riesgos en seguridad de la información de acuerdo con el apetito de riesgo de la empresa.

11.5.6. Estándares de la Política del Tratamiento y Gestión del Riesgo en Seguridad de la Información

Periódicamente se debe realizar una valoración del riesgo para contemplar los cambios en los requisitos de seguridad y la situación de riesgo, tales como cambio en los activos, las amenazas, las vulnerabilidades y los impactos. Se debe decidir cuándo un riesgo es aceptable, ya sea por motivos de objetivos de negocio o por costes no rentables. Los posibles tratamientos a los riesgos identificados incluyen:

- Evitar el riesgo.
- Disminuir la probabilidad de ocurrencia.
- Disminuir el impacto.
- Transferir los riesgos.
- Retener los riesgos.

11.6. SEGURIDAD DEL PERSONAL

11.6.1. Política de Responsabilidad del Personal

El Rol de Gestión Humana debe notificar al Rol de Tecnología todas las novedades del personal directo e indirecto tales como ingresos, traslados, delegaciones, retiros y vacaciones.

11.6.2. Estándares de la Política de Seguridad del Personal

11.6.2.1. Seguridad previa a la contratación del personal y personal provisto por terceros.

Para toda persona que ingrese a la compañía, El Rol de Gestión Humana debe asegurar las responsabilidades sobre seguridad de manera previa a la contratación. Esta tarea debe reflejarse en una adecuada descripción del cargo y en los términos y condiciones de la contratación.

11.6.2.2. Seguridad durante el contrato.

El Rol de Gestión Humana debe desarrollar un programa efectivo y continuo de concientización de protección de la información para todo el personal. También se requiere de capacitación específica en administración de riesgos tecnológicos para aquellos individuos que están a cargo de responsabilidades especiales de protección y los conceptos básicos con que debe cumplir todo colaborador. Es responsabilidad y deber de cada colaborador de PLASPEL SAS asistir a los cursos de concientización en seguridad de la información que la empresa programe y aplicar la seguridad según las políticas y los procedimientos establecidos por la empresa.

11.6.2.3. Finalización o cambio de puesto.

El Rol de Gestión Humana debe asegurar que todos los funcionarios, consultores, contratistas, terceras partes, que salgan de la empresa o cambien de puesto de trabajo, hayan firmado un acuerdo de confidencialidad, cuyo cumplimiento será vigente hasta que PLASPEL SAS lo considere conveniente, incluso después de la finalización del puesto de trabajo o del

contrato. El Rol de Gestión Humana se asegurará que la salida o movilidad de los funcionarios, contratistas o terceros sea gestionada hasta la completa devolución de todos los activos y retirada de los derechos de acceso.

11.7. SEGURIDAD FÍSICA, MEDIOAMBIENTAL Y DEL ENTORNO

11.7.1. Política de Seguridad Física y del Entorno

El centro de procesamiento de datos y cuarto de equipos tecnológico, deben de estar en áreas protegidas físicamente contra el acceso no autorizado, daño o interferencia y deben cumplir con las políticas de seguridad física.

11.7.1.1. Estándares de la Política de Seguridad Física y del Entorno

11.7.1.1.1. Controles de acceso físico.

El acceso a áreas TIC restringidas sólo se debe permitir para:

- Desarrollo de operaciones tecnológicas.
- Tareas de aseo (monitoreado por personal del Rol de Gestión de Tecnología).
- Pruebas de equipos.
- Almacenamiento de equipos.
- Implementación o mantenimiento de los controles ambientales.

El Rol de Tecnología 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. Si algo no es de su competencia para este objetivo, debe gestionarlo. Debe velar porque los recursos de la plataforma tecnológica de PLASPEL SAS ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas. 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. Está encargada de la adquisición, instalación y protección ambiental de los equipos y componentes Tecnológicos de las Empresas. También está encargada de la instalación, configuración y mantenimiento de dispositivos de control ambiental en los centros de cómputo. Debe preparar y oficializar cronogramas de mantenimiento preventivo de los equipos y componentes bajo su responsabilidad, con revisión anual de cumplimiento y debe coordinar su ejecución con el Administrador del centro de cómputo. Debe establecer un cronograma de pruebas de los sistemas de control ambiental teniendo en cuenta el tipo de sistema, criticidad e impacto de cada centro de cómputo.

Los responsables de Rol 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 su áreas. Deben autorizar cualquier ingreso temporal a sus áreas, evaluando la pertinencia del ingreso; así mismo, deben delegar en personal del Rol el registro y supervisión de cada ingreso a sus áreas. Deben velar porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas solo sean utilizadas por los funcionarios autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos no sean transferidos a otros funcionarios de la compañía.

Los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados. Deben portar el carnet que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la compañía; en caso de pérdida del carnet o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible. No deben intentar ingresar a áreas a las cuales no tengan autorización.

Todo evento reportado por un sistema de control ambiental conectado al panel de alarmas del Rol de seguridad debe ser notificado por todo funcionario al Rol de Tecnología.

Como mínimo cada 30 días debe efectuarse labores de aseo en los centros de cómputo. Únicamente personal autorizado por el Rol de Tecnología debe ingresar al centro de cómputo a realizar estas labores. Dicho Rol debe verificar de manera periódica que el centro de cómputo se encuentre en perfecto estado de limpieza y organización.

En los centros de cómputo y centros de cableado no deben alojarse equipos ni repuestos obsoletos, desechos o elementos electrónicos y en general cualquier material combustible como ropa, papelería, cajas; que puedan generar algún tipo de evento negativo que afecte el componente Tecnológico del centro de cómputo.

11.7.1.1.2. Escritorio limpio.

La implementación de una directriz de escritorio limpio permitirá reducir el riesgo de acceso no autorizado o daño a medios y documentos. Los computadores deben bloquearse después de diez (10) minutos de inactividad, el usuario tendrá que autenticarse antes de reanudar su actividad. Todos los funcionarios, consultores, contratistas, terceras partes, deben bloquear la sesión al alejarse de su computador.

11.7.1.1.3. Seguridad de los equipos.

Para prevenir la pérdida de información daño o el compromiso de los activos de información y la interrupción de las actividades de PLASPEL SAS, los equipos deben estar conectados a la toma regulada destinada para tal fin.

11.7.1.1.4. Retiro de equipos.

Se deben tener en cuenta los procesos de instalación y retirada del equipo, de tal manera que estos se hagan de forma controlada y segura. La protección de los equipos, incluso cuando se utilizan fuera de la oficina, es necesaria para reducir el riesgo no autorizado de acceso a la información y para protegerlo contra pérdida o robo.

11.8. CONTROL DE ACCESO A LA INFORMACIÓN

11.8.1. Política de Control de Acceso a la Información

El Rol de Tecnología, conforme la clasificación de activos de información, debe implementar las medidas de seguridad aplicables según el caso, con el fin de evitar la adulteración, pérdida, fuga, consulta, uso o acceso no autorizado o fraudulento. El control de acceso de datos e información sensible se debe basar en el principio del menor privilegio, lo que implica que no se otorgará acceso a menos que sea explícitamente permitido. 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.

Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de PLASPEL SAS, deben contar con el formato de creación de cuentas de usuario 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 Compañía deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

11.8.2. Estándares de Política de Control de Acceso a la Información

11.8.2.1. Gestión de acceso a usuarios.

El Rol de Tecnología establecerá procedimientos formales para controlar la definición de perfiles y la asignación de derechos de acceso a los usuarios, previamente definidos por el Rol responsable del proceso. Dichos procedimientos deben cubrir todas las etapas del ciclo de vida del usuario, desde su registro inicial hasta la eliminación o desactivación del registro a quienes no necesiten el acceso. Se debe brindar atención y seguimiento especial, donde sea apropiado, a la necesidad del control de asignaciones de accesos privilegiados. Debe establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información del instituto, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario. Debe definir lineamientos para la configuración de contraseñas que aplicaran sobre la plataforma tecnológica, los servicios de red y los sistemas de información de PLASPEL SAS; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros. 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 funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo. Debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.

11.8.2.2. Registro de usuarios.

Todos los usuarios deben tener una identificación única personal o jurídica, que se utilizará para el seguimiento de las actividades de responsabilidad individual o jurídica. Las actividades habituales de usuario no deben ser desempeñadas a través de cuentas privilegiadas. En circunstancias excepcionales, por beneficio de la compañía, se podrá usar un identificador compartido, para un grupo de usuarios con trabajo específico; este debe ser autorizado y debidamente aprobado por el Rol de Tecnología. El usuario debe tener autorización de la

respectiva empresa para el uso del sistema o servicio de información. Se debe verificar que el nivel de acceso otorgado sea adecuado para los propósitos de la empresa y conserven una adecuada segregación de funciones. Adicionalmente, deben tomar y certificar la formación y así garantizar el uso adecuado del sistema o servicio de información.

11.8.2.3. Responsabilidades del usuario.

Una seguridad efectiva requiere la cooperación de los usuarios autorizados, quienes deben saber sus responsabilidades para el mantenimiento de controles efectivos al acceso, en particular, aquellos con referencia al uso de contraseñas, El Rol de Tecnología implementará los procedimientos necesarios que permitan controlar la creación, modificación, desactivación y eliminación de usuarios, administración de contraseñas y permisos de acceso a los recursos tecnológicos y a la información. Adicionalmente, es necesario implementar un procedimiento de revisión periódica de los permisos de acceso de los usuarios. Los funcionarios, contratistas y terceros entienden las condiciones de acceso y deben mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo únicamente entre los miembros de este. Esta declaración puede ser incluida en los términos y condiciones laborales. Igualmente deben cumplir las buenas prácticas en la selección y uso de la contraseña.

11.8.2.4. Control de acceso a la red.

Únicamente se debe proporcionar a los funcionarios el acceso a los servicios para los que específicamente se les haya autorizado su uso. Se deben utilizar métodos apropiados de autenticación para el control de acceso a los usuarios remotos. Se deben implantar controles adicionales para el acceso por redes inalámbricas. Se debe establecer una adecuada segregación de redes, separando los entornos de red de usuarios y los servicios.

11.8.2.5. Control de acceso a las aplicaciones y sistemas de información.

El uso de programas que puedan ser capaces de invalidar los controles del sistema y de la aplicación, deben estar restringidos y estrictamente controlados. Las sesiones inactivas deben cerrarse después de un período de inactividad definido y se deben usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo. Las cuentas de usuario de herramientas o productos que vengan por omisión se deben deshabilitar inmediatamente después de la instalación de los sistemas o software. Las contraseñas predeterminadas por el proveedor se deben cambiar inmediatamente después

de la instalación de los sistemas o software. El Rol de Tecnología debe integrar las aplicaciones con el Directorio Activo.

Los propietarios de los activos de información 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. Deben monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

El Rol de Tecnología 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. Debe establecer un procedimiento para la asignación de accesos a los sistemas y aplicativos. 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 asegurar, mediante los controles necesarios, que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error. Debe establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción. Debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

Los desarrolladores 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 certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas. 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 deshabilitar 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 asegurar que si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los

aplicativos, los cuales deben tener un periodo de validez establecido; se deben forzar el cambio de las contraseñas temporales después de su utilización. Deben certificar que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información. Deben asegurar la re-autenticación de los usuarios antes de la realización de operaciones críticas en los aplicativos. 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. Deben establecer que periódicamente se re-valide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados.

11.9. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

11.9.1. Política de Gestión de incidentes de Seguridad de la Información

Todos los funcionarios, consultores, contratistas, terceras partes, deben anotar y comunicar cualquier punto débil que hayan observado o que sospechen que exista en los sistemas o servicios a través de la mesa de servicios.

11.9.2. Estándares de la Política de Gestión de Incidentes de Seguridad de la Información

11.9.2.1. Notificación de eventos y debilidades de seguridad de la información.

El Rol de Tecnología debe asegurarse de que los eventos y los puntos débiles de seguridad de la información asociados con los sistemas de información, se comunican de forma que sea posible emprender acciones correctivas. Se debe establecer un procedimiento formal de comunicación de eventos de seguridad de la información, junto con un procedimiento de respuesta y escalado de incidentes, que determine la respuesta que debe darse cuando se recibe un informe de un evento de seguridad de la información.

11.9.2.2. Gestión de incidentes de seguridad de la información.

Se deben establecer responsabilidades y procedimientos para tratar los eventos y los puntos débiles de seguridad de la información de forma efectiva. Una vez que se hayan comunicado a través de un proceso de mejora continua, el grupo de resolución de problemas se encargará de analizar la causa y evaluar conforme al proceso de gestión de problemas. Cuando se detecta por primera vez un evento de seguridad de la información, puede que no resulte evidente si dicho evento tendrá como consecuencia una acción legal. Por este motivo, existe el peligro que se destruyan de forma intencional o accidental de las pruebas necesarias antes de tomar conciencia de la gravedad del incidente. Se debe hacer uso de los servicios jurídicos de PLASPEL SAS y/o de los entes de control en las primeras fases de cualquier acción legal que se esté considerando, así como asesorarse de las pruebas necesarias. Cuando una acción contra una persona u organización, después de un incidente de seguridad de la información, implique medidas legales (tanto civiles como penales), deberían recopilarse pruebas, que deberían conservarse y presentarse de manera que se ajusten a las normas legales vigentes. A la hora de la recopilación de las pruebas, se preservará la cadena de custodia y se utilizarán herramientas y procedimientos aceptados de análisis forenses.

11.10. GESTIÓN DE SEGURIDAD PARA TELECOMUNICACIONES E INFRAESTRUCTURA DE TIC

11.10.1. Política de Gestión de Telecomunicaciones e Infraestructura de TIC

El Rol de Tecnología debe proveer el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación, a través de una Gestión de Telecomunicaciones e Infraestructura de TIC efectiva y eficiente.

11.10.2. Estándares de la Política de la Política de Gestión de Telecomunicaciones e Infraestructura de TIC

11.10.2.1. Procedimientos y responsabilidades de operación.

El Rol de Tecnología debe definir y documentar claramente las responsabilidades para el manejo y operación de instalaciones de computadores y redes, apoyadas por instrucciones operacionales apropiadas incluyendo procedimientos de respuesta en caso de incidentes.

También debe definir controles que garanticen la apropiada operación tecnológica. Estos controles deben incluir como mínimo los siguientes procedimientos:

- Copias de seguridad.
- Verificación de cintas.
- Recuperación de datos y reversión de cambios.
- Administración de sistemas de antivirus.
- Administración de usuarios y contraseñas.
- Administración de acceso a los recursos.
- Administración de acceso remoto.
- Medición de desempeño.
- Capacidad y disponibilidad de los recursos de TI.
- Gestión de pistas de auditoria y sistemas de registro de información.
- Aseguramiento de plataformas.

11.10.2.2. Gestión del Cambio.

El Rol de Tecnología debe implementar los controles necesarios que permitan garantizar la segregación de funciones y un adecuado seguimiento a los cambios efectuados a los activos críticos de TI. La documentación debe incluir, entre otros:

- Persona que solicita el cambio.
- Responsable de autorización.
- Descripción del cambio.
- Justificación del cambio para el negocio.
- Lista de chequeo para evaluación de riesgos, sistemas y/o dispositivos comprometidos. o Nivel de impacto.
- Pruebas, aprobación revisiones de post-implementación. o Capacitación, cuando sea necesario.

11.10.2.3. Segregación de funciones.

Las tareas y responsabilidades propias de gestión de tecnología, se deben segregar para reducir e impedir las oportunidades de acceso no autorizado a la red y cualquier modificación o mal uso de los activos de los sistemas de información. Se prestará especial cuidado que una persona no pueda por si misma acceder, modificar o utilizar los activos, sin previa autorización.

11.10.2.4. Separación de Ambientes.

Cuando aplique los ambientes de desarrollo, pruebas y producción deben estar separados para reducir los riesgos de acceso o cambios no autorizados, prevenir fallos e implementar controles.

11.10.2.5. Planificación y Aceptación.

Se deben definir los requisitos de capacidad futura, con el fin de reducir el riesgo a una sobrecarga del sistema. Los requisitos operativos de sistemas nuevos se deben establecer, documentar y probar antes de su aceptación. Los requisitos de restitución para los servicios apoyados por diferentes aplicaciones se deben coordinar y revisar frecuentemente. Los administradores de TI deben estar alerta a los riesgos asociados a estas tecnologías, así mismo considerar la toma de medidas especiales para su prevención o detección.

11.10.2.6. Protección contra el código malicioso.

El Rol de Tecnología debe implementar controles de detección, prevención y recuperación para la protección frente al código malicioso. 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 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.

Los usuarios deben ser conscientes de los peligros de los códigos maliciosos. En PLASPEL SAS no está permitido el uso de software no licenciado y su instalación en cualquiera de los equipos de la compañía. Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por

el Rol de Tecnología; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios. 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, el Rol de Tecnología tome las medidas de control correspondientes.

11.10.2.7. Copias de seguridad.

Se deben hacer copias de respaldo de la información y del software. Para garantizar la integridad y disponibilidad, se debe hacer su comprobación regular de los mecanismos y la información en conformidad con la política de respaldo acordada, conservando los niveles de confidencialidad requeridos. El Rol de Tecnología debe almacenar las copias de seguridad por fuera de las instalaciones de PLASPEL SAS con el fin de garantizar su recuperación en caso de un evento mayor en la sede principal.

La Compañía 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 del Rol de Tecnología, 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.

El Rol de Tecnología, a través de sus funcionarios, 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.

Los responsables de los recursos obligatorios, los propietarios de los recursos tecnológicos y sistemas de información deben definir, en conjunto con el Rol de Tecnología, las estrategias

para la generación, retención y rotación de las copias de respaldo de los activos de información.

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

11.10.2.8. Gestión de seguridad en registro de eventos y monitoreo de recursos de los sistemas de información

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

El Auditor Interno debe determinar los periodos de retención de los registros (logs) de auditoria de los recursos tecnológicos y los sistemas de información del instituto. 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.

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

11.10.2.9. Gestión de seguridad en periféricos y medios de almacenamiento

El Comité de Seguridad de la Información debe establecer las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica de PLASPEL SAS Debe autorizar el uso de periféricos o medios de almacenamiento en la plataforma tecnológica del instituto de acuerdo con el perfil del cargo del funcionario solicitante.

El Rol de Tecnología debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica del instituto, de acuerdo con los lineamientos y condiciones establecidas. Debe generar y aplicar lineamientos para la disposición segura de

los medios de almacenamiento del instituto, ya sea cuando son dados de baja o re-asignados a un nuevo usuario.

Los funcionarios y el personal provisto por terceras partes deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por el Rol de Tecnología. No deben modificar la configuración de periféricos y medios de almacenamiento establecidos. Son responsables por la custodia de los medios de almacenamiento institucionales asignados.

11.10.2.10. Gestión de seguridad con criptografía

El Rol de Tecnología debe establecer que periódicamente se re-valide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados. Debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos. Debe desarrollar y establecer un procedimiento para el manejo y la administración de llaves de cifrado. Debe desarrollar y establecer estándares para la aplicación de controles criptográficos.

Los desarrolladores deben cifrar la información reservada o restringida y certificar la confiabilidad de los sistemas de almacenamiento de dicha información. Deben asegurarse que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos.

11.10.2.11. Gestión de seguridad en la operación

El Rol de Tecnología, encargada de la operación y administración de los recursos tecnológicos que apoyan los procesos de PLASPEL SAS, asignará funciones específicas a sus funcionarios, 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. Proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información del instituto, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida. Debe efectuar, a través de sus funcionarios, la documentación y actualización de

los procedimientos relacionados con la operación y administración de la plataforma tecnológica. Debe proporcionar a sus funcionarios 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. 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. Debe emitir concepto y generar recomendaciones acerca de las soluciones de seguridad seleccionadas para la plataforma tecnológica.

11.10.2.12. Gestión de seguridad en el intercambio de la información

PLASPEL SAS, 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. El instituto 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.

El Rol de Tecnología, con el apoyo solicitado de las Áreas competentes, debe definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre el instituto y tercera 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 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 del instituto que les ha sido entregada en razón del cumplimiento de los objetivos misionales. 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.

El Comité de Seguridad de la Información debe definir y establecer el procedimiento de intercambio de información con los diferentes terceros que, hacen parte de la operación, reciben o envían información de los beneficiarios del instituto, 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 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.

Los propietarios de los activos de información deben velar porque la información 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 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 así como del procedimiento de intercambio de información.

El usuario remitente o receptor de información física, con el apoyo del Coordinador Administrativo, 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, y que estos permitan ejecutar rastreo de las entregas.

El tercero con quien se intercambia información debe darle manejo adecuado a la información recibida, en cumplimiento de las Políticas de seguridad del instituto, de las condiciones contractuales establecidas y del Procedimiento de intercambio de información. Debe 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.

Los responsables de Rol deben impartir instrucciones claras sobre qué información puede transmitirse por qué canal de comunicación.

11.10.2.13. Gestión de seguridad en las comunicaciones

El Rol de Tecnología establecerá, a través del Rol de Tecnología, 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 del instituto. 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 el instituto. 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 del instituto, acogiendo buenas prácticas de configuración segura. Debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos por el instituto en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos. Debe instalar protección entre las redes internas y cualquier red externa, que este fuera de la capacidad de control y administración del instituto. Debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos

11.10.2.14. Gestión de seguridad en vulnerabilidades

El Rol de Tecnología 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. 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

El Rol 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 Rol 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.

El Comité de Seguridad de la Información debe revisar, valorar y gestionar las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación.

11.10.2.15. Gestión de seguridad en protección de los datos de prueba

El Rol de Tecnología del protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción. 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.

11.10.2.16. Gestión de seguridad con terceras partes

PLASPEL SAS 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 funcionarios 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

El Rol Jurídica, en conjunto con el Comité de Seguridad de la Información 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.

El Rol de Tecnología debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos del instituto. 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. Debe evaluar y aprobar los accesos a la información del instituto 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.

Los Supervisores de contratos con terceros deben divulgar las políticas, normas y procedimientos de seguridad de la información 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.

11.10.2.17. Gestión de seguridad en incidentes y su correspondiente reporte

PLASPEL SAS promoverá entre los funcionarios 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. 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. 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.

Los propietarios de los activos de información deben informar al Comité de Seguridad de la Información, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

El Comité de Seguridad de la Información 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 nueva ocurrencia. Debe 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 (para esto aplica el reporte de eventos de riesgo operativo). Debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

Todos los funcionarios de PLASPEL SAS y el 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 funcionarios deben notificarlo a la Oficina de Riesgo para que se registre y se le dé el trámite necesario.

11.10.2.18. Gestión de seguridad en Redundancia

El Comité de Seguridad de la Información debe analizar y establecer los requerimientos de redundancia para los sistemas de información críticos para el instituto y la plataforma tecnológica que los apoya. Debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos.

El Rol de Tecnología debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad del instituto.

11.10.2.19. Gestión de seguridad en Plan de Continuidad del Negocio

PLASPEL SAS, proporcionará los recursos suficientes para proporcionar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten en el instituto 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. La Compañía mantendrá canales de comunicación adecuados hacia funcionarios, proveedores y terceras partes interesadas.

El Comité de Continuidad debe reconocer las situaciones que serán identificadas como emergencia o desastre para el instituto, 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. Debe seleccionar las estrategias de recuperación más convenientes para el instituto. 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.

El Comité de Seguridad de la Información debe 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 al Gerente General.

Los responsables de Rol deben 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.

11.10.2.20. Gestión de seguridad en la prestación de servicios de terceras partes

PLASPEL SASL, mantendrá 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.

El Rol de Tecnología 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 del instituto. Debe verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

El Comité de Seguridad de la Información y el Rol cliente del contrato, deben 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

11.10.2.21. Gestión de seguridad en conexión remota

El Rol de Tecnología, debe analizar y aprobar los métodos de conexión remota a la plataforma tecnológica de PLASPEL SAS Debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de PLASPEL SAS Debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas. Debe verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de PLASPEL SAS de manera permanente.

El Rol de Auditoria Interna debe, dentro de su autonomía, realizar auditorías sobre los controles implantados para las conexiones remotas a la plataforma tecnológica de PLASPEL SAS

Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de PLASPEL SAS y deben acatar las condiciones de uso establecidas para dichas conexiones. Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y, bajo ninguna circunstancia, en computadores público, de hoteles o cafés internet, entre otros.

11.10.2.22. Gestión de seguridad en tokens

PLASPEL SAS, proveerá las condiciones de manejo de los tokens de seguridad para los procesos que los utilizan y velará porque los funcionarios hagan un uso responsable de estos.

Cada Rol usuaria de tokens de seguridad debe asignar un funcionario administrador de los mismos con la potestad para autorizar las solicitudes de acceso.

Los Administradores de los tokens de seguridad deben procesar las solicitudes de dichos tokens según los requerimientos de cada entidad proveedora de éstos y adjuntar la documentación necesaria. Deben recibirlos y realizar la activación necesaria en los respectivos portales o sitios de uso para poder realizar operaciones por medio de ellos. Deben crear los usuarios y perfiles en cada portal o sitio de uso, según las actividades a realizar por cada funcionario creado. Deben entregar a los funcionarios designados los usuarios y seriales de los dispositivos que le son asignados para su uso, formalizando la entrega por medio de acta y tula (o sobre) de seguridad para custodia de los mismos. Deben dar avisos a las entidades

emisoras en caso de robo o pérdida de estos con el fin de efectuar el bloqueo respectivo y la reposición de los mismos. Deben realizar el cambio de estos, cuando se presente mal funcionamiento, caducidad, cambio de funciones o cambio del titular, reportando a la entidad emisora y devolviendo los dispositivos asignados.

Los Usuarios de los tokens de seguridad deben contar con una cuenta de usuario en los portales o sitios de uso de los mismos; dichos tokens harán parte del inventario físico de cada usuario a quien se haya asignado. deben devolver el token asignado en estado operativo al Administrador de los tokens cuando el vínculo laboral con PLASPEL SAS se dé por terminado o haya cambio de cargo, para obtener el paz y salvo, el cual será requerido para legalizar la finalización del vínculo con el instituto. Deben notificar al Administrador de los tokens en caso de robo, pérdida, mal funcionamiento o caducidad para que este a su vez, se comunique con las entidades emisoras de dichos tokens. No deben permitir que terceras personas observen la clave que genera el token, así como no deben aceptar ayuda de terceros para la utilización del token. Deben responder por las transacciones electrónicas que se efectúen con la cuenta de usuario, clave y el token asignado, en el desarrollo de las actividades como funcionarios del PALSPEL SAS En caso de que suceda algún evento irregular con los tokens los usuarios deben asumir la responsabilidad administrativa, disciplinaria y económica. Deben mantener los tokens asignados en un lugar seco y no introducirlos en agua u otros líquidos. Deben evitar exponer los tokens a campos magnéticos y a temperaturas extremas. Deben evitar que los tokens sean golpeados o sometidos a esfuerzo físico. No deben abrir los tokens, retirar la batería o placa de circuitos, ya que ocasionará su mal funcionamiento. No deben usar los tokens fuera de las instalaciones de PLASPEL SAS para evitar pérdida o robo de estos

11.10.2.23. Gestión de seguridad en las redes.

Se le debe dar atención especial al manejo de la seguridad en redes, la cual puede extenderse más allá de los límites físicos de PLASPEL SAS

Procedimientos y medidas especiales se requieren para proteger el paso de información sensible a redes de dominio público.

El Rol de Tecnología debe garantizar que los proveedores de servicios de red implementan medidas en cumplimiento con las características de seguridad, acuerdos de niveles de servicio y requisitos de gestión. Se deben establecer controles especiales para salvaguardar la integridad y confidencialidad de los datos que pasan por redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectadas, igualmente se debe garantizar la disponibilidad de los servicios de red y computadores conectados.

11.10.2.24. Servicios de Comercio Electrónico.

Se debe realizar una evaluación para identificar el riesgo asociado con el uso de servicios de comercio electrónico, incluyendo las transacciones en línea y los requisitos para los controles. Se debe considerar la integridad y la disponibilidad de la información publicada electrónicamente a través de sistemas disponibles al público.

11.10.2.25. Monitoreo de uso del sistema.

El nivel de monitoreo necesario para los servicios se determinará mediante una evaluación de riesgos. PLASPEL SAS cumplirá los requisitos legales que se apliquen en sus actividades de monitoreo. Se deben registrar las actividades tanto del operador como del administrador del sistema. Las actividades a monitorear incluyen: operaciones privilegiadas, acceso no autorizado y alertas o fallas del sistema, entre otras.

11.10.2.26. Registros de Auditoría.

Se deben elaborar y mantener durante un período acordado, los registros de auditoría de las actividades de usuario, de operación y administración del sistema.

11.10.2.27. Protección de la información de registro.

Los servicios y la información de la actividad de registro se deben proteger contra el acceso o manipulación no autorizados.

11.10.2.28. Tratamiento de medios con información.

Se deben controlar los medios y proteger para prevenir la revelación, modificación, eliminación o destrucción no autorizada de los activos y la interrupción de las actividades del negocio. El Rol de Tecnología debe implementar los controles que permitan garantizar que la eliminación de cualquier dispositivo o componente tecnológico que contenga información sensible, sean destruidos físicamente, o bien que la información sea destruida, borrada o sobrescrita, mediante técnicas que no hagan posible la recuperación de la información original, en lugar de utilizar un borrado normal o formateado.

11.10.2.29. Protección de Contraseñas

- El correo electrónico no es un medio seguro. Por esta razón no se debe enviar la contraseña por este medio, ni mencionarla en una conversación.
- No se deben almacenar contraseñas en formato legible en archivos tipo "batch", scripts de login automáticos, macros de software, teclas de función de terminales, computadores sin control de acceso o en otros sitios donde personas no autorizadas puedan descubrirlos y utilizarlos.
- Cada contraseña es de uso personal e intransferible. Los funcionarios y terceros que trabajan para PLASPEL SAS no han de revelar la contraseña de su cuenta a otros funcionarios y/o terceros.
- Está prohibido intentar ingresar a los servicios de cómputo y comunicaciones por medio de la cuenta de otro funcionario.
- Los funcionarios y terceros que trabajan para PLASPEL SAS deben notificar en forma inmediata al Comité de Seguridad de la Información si sospechan que alguien ha obtenido acceso sin autorización a su cuenta. La contraseña se debe cambiar en forma inmediata.
- No se debe permitir que individuos que no sean miembros de PLASPEL SAS obtengan acceso a los servicios de cómputo y comunicaciones de las empresas. Todos los funcionarios y terceros (contratistas, proveedores de servicios y outsourcing) deben velar porque este tipo de situaciones no se presenten al interior de PLASPEL SAS
- Cada usuario es responsable por la custodia de su contraseña y cuenta. Debe evitar en lo posible digitar la contraseña mientras alguna persona está observando lo que escribe en el teclado. Es una norma tácita de buen usuario no mirar el teclado mientras alguien teclea su contraseña.

11.10.2.30. Control de virus

Hace parte de la política de Seguridad de la Información de PLASPEL SAS la no tolerancia a la propagación de virus, tratados con medidas eficientes a lo largo del documento

11.10.2.31. Confidencialidad de la Información

Hace parte de la política de Seguridad de la Información de PLASPEL SAS la gestión de información de forma confidencial, tratada con medidas eficientes a lo largo del documento

11.10.2.31. Verificación del Cumplimiento

Hace parte de la política de Seguridad de la Información de PLASPEL SAS la gestión de verificación del cumplimiento de todas las normas requeridas en materia de Seguridad de la Información, tratada con medidas eficientes a lo largo del documento

11.10.2.32. Equipo sin uso

Los funcionarios y contratistas deben adoptar como mínimo las siguientes prácticas al dejar desatendido su equipo:

- Dejar ubicado el equipo en una zona segura
- Bloquear sus equipos de cómputo con protector de pantalla protegido con contraseña cuando dicho equipo vaya a estar desatendido por más de tres (3) minutos.

11.10.2.33. Respaldo – Back Up de la Información

Hace parte de la política de Seguridad de la Información de PLASPEL SAS la gestión de copias de seguridad de la información, tratada con medidas eficientes a lo largo del documento

11.10.2.34. Eliminación de Derechos de Acceso

En el caso de retiro voluntario, despido, traslado u otro tipo de actividad asociada con la culminación o modificación del contrato, acuerdo de servicio u otro tipo de acuerdo escrito

de los funcionarios de las empresas o terceros que cuenten con privilegios de acceso, estos derechos deben ser removidos/inactivados o actualizados según se establezca.

Debe efectuarse el siguiente procedimiento:

- El Rol de Gestión Humana debe reportar la novedad (solo para retiro de personal contratado directamente, a través de empresa temporal o por servicios) de funcionarios de forma inmediata que conozca la novedad del empleado.
- El Rol de Tecnología debe efectuar los ajustes correspondientes. El plazo máximo para eliminar/inactivar o modificar los accesos de un funcionario es no mayor a 3 días calendario desde que se reportó la novedad.
- El Comité de Seguridad de la Información y el Auditor Interno también efectuarán revisiones en los componentes y activos de Información con el fin de validar el cumplimiento de la política.

11.10.2.35. Seguridad de los equipos fuera de la compañía

- Los computadores portátiles no se deben utilizar en los hogares para conectarse a Internet u otras redes si no existen controles contra virus y firewall de computador personal instalado, configurado en forma apropiada y en constante funcionamiento.

- Durante cualquier desplazamiento, los equipos (y medios de almacenamiento) no se deben dejar desatendidos. Los computadores portátiles se deben llevar como equipaje de mano custodiados en forma permanente.

- Los equipos de cómputo (sin importar su propietario) utilizados fuera de PLASPEL SAS y en funciones propias de la Compañía, deben ser exclusivamente utilizados para brindar apoyo al negocio y deben estar sujetos a un grado equivalente de protección a los equipos que se encuentran dentro de las instalaciones de las empresas.

11.10.2.36. Destrucción de Medios

Todos los equipos de cómputo, dispositivos Tecnológicos y cualquier tipo de medio electrónico que contenga Información crítica para el negocio de PLASPEL SAS debe ser revisado, analizado y la información contenida eliminada de manera segura antes que el medio sea reasignado o destruido cuando los requerimientos del negocio no requieran de su uso.

El Rol de Tecnología es quien establece los diferentes responsables de la destrucción de los medios según sea el tipo y su función (medios de backup, equipos de cómputo, etc.). Debe establecer procedimientos para la destrucción de los medios y deben estar sujetos a aprobación por parte del Comité de Seguridad de la Información. Todo proceso de destrucción de medios debe ser formalizado y registrado mediante el memorando de destrucción de medios.

Previamente a la destrucción de un medio magnético el Funcionario encargado debe verificar si es necesario efectuar una copia de seguridad de la Información que se encuentra en el medio previo a su destrucción o reasignación

Cuando un equipo de cómputo sea entregado a un tercero o reasignado y éste cuente con unidad de almacenamiento (disco duro) debe ser revisado por el Rol de Tecnología y la información debe ser borrada de tal forma que no pueda ser recuperable. En caso que el dispositivo no tenga unidad de almacenamiento (ej: equipos de comunicaciones) debe ser reinicializado a la configuración que trae de fábrica.

La información almacenada en dispositivos de almacenamiento como discos duros y unidades de USB debe ser eliminada mediante el uso de herramientas especializadas que permitan formatear las particiones de manera segura con el fin que la información previamente almacenada no pueda ser restaurada. La herramienta a utilizar es aprobada por el Comité de Seguridad de la Información.

En caso que los medios sean cedidos o donados a un tercero para fines benéficos, estos deben seguir los lineamientos aquí descritos de acuerdo a lo estipulado en esta política.

El Comité de Seguridad de la Información efectuará revisiones periódicas al cumplimiento de lo consignado en esta política.

11.10.2.37. Control de cambios tecnológicos.

El Rol de Tecnología establece dos tipos de cambio: Los cambios programados u operativos y los cambios de urgencia.

Cambios programados: Son cambios que se deben implementar como resultado de un requerimiento, actualización o mejora de un componente tecnológico.

Cambios de urgencia: Este tipo de cambios requieren atención prioritaria y/o inmediata y pueden justificarse fuera del ciclo normal de cambios. Pueden ser generados debido a una falla o mal funcionamiento de un componente de Tecnología de Información y que puede

impactar de manera significativa los procesos del negocio. Este tipo de cambios pueden ser ejecutados por El Rol de Tecnología correspondiente previo al aval del designado. Una vez sean implementados deben ser oficializados y documentados en las siguientes 36 horas hábiles de haber sido aplicados.

Debe existir un procedimiento formal de control de cambios de acuerdo al tipo de cambio y debe seguirse para controlar las modificaciones al componente de TI. Ningún cambio se puede implementar sin previo cumplimiento a lo establecido en el procedimiento.

Todo cambio a la plataforma Tecnológica o Sistemas de Información debe estar sujeto a aprobación a priori a la aplicación del mismo por el Rol funcional involucrada y afectada por el cambio. La conformación del "grupo de aprobación de control de cambios" dependerá del tipo de componente, criticidad e impacto que pueda generar el cambio. Los funcionarios involucrados en la aprobación corresponden a la matriz de responsables de Sistemas de Información e Infraestructura.

Todo cambio debe ser probado en un ambiente separado antes de su puesta en producción. El resultado de las pruebas debe ser documentado por el administrador de la Plataforma o por el Rol funcional en el caso de Sistemas de Información.

Cada Administrador de la plataforma tecnológica o Sistema de Información debe llevar un registro histórico de los cambios aplicados a cada componente de TI que administra.

Los cambios a la información de las base de datos deben estar aprobados por el Rol funcional correspondiente y por tanto no está permitido crear o modificar datos de parte de funcionarios del Rol de Tecnología Informática sin previa solicitud y autorización.

Cualquier aplicación de un cambio en la plataforma de TI que afecte los servicios de PLASPEL SAS debe ser informada a un funcionario de cada Compañía afectada antes de efectuar el cambio. Este funcionario es designado por el Rol de Tecnología.

11.10.2.38. Monitoreo de Componentes Tecnológicos.

Todo proceso, actividad y servicio del negocio que esté soportado por Tecnología de Información debe ser analizado por la el Rol de Tecnología. Los Administradores de cada Plataforma componente deben establecer los requerimientos de capacidad de los sistemas involucrados en la etapa de especificación de requerimientos de proceso, actividad o servicio del negocio. Para tal fin se debe tener en cuenta como mínimo los siguientes criterios de evaluación de requerimientos de capacidad:

- Tamaño y tipo de servicio prestado por el Componente Tecnológico.
- Estimación de la capacidad requerida para la prestación del servicio de manera adecuada y eficiente.
- Efectuar un análisis de la información y los datos a manejar por el sistema.
- Establecer el nivel de impacto de la implementación de los sistemas y las operaciones.

Todos los componentes críticos deben ser revisados periódicamente, teniendo en cuenta como mínimo los siguientes factores de monitoreo:

- Capacidad
- Desempeño
- Disponibilidad

El Rol de Tecnología debe establecer la frecuencia de revisión, los indicadores, la métrica y los umbrales definidos para cada Componente Tecnológico a fin de determinar su capacidad y desempeño.

11.10.2.39. Controles en Redes

Todos los dispositivos sin excepción alguna que sean ingresados a las redes de datos Corporativas (incluyendo equipos de cómputo, impresoras, escáner, dispositivos de comunicaciones, entre otros) deben ser previamente registrados y configurados por el Rol de Tecnología.

Cuando un componente Tecnológico es registrado para uso en las redes Corporativas un nombre de red y dirección IP le será asignado de acuerdo al mecanismo establecido por el Rol de Tecnología. La información básica del propietario del componente, descripción y función debe ser registrada por el Administrador de dicho Componente o a quien designe.

La definición y diseño del direccionamiento de las redes, así como la aprobación de asignación de direcciones IP fijas en la red es responsabilidad del Rol de Tecnología.

Todo Componente Tecnológico que sea ingresado a las redes Corporativas debe cumplir con los requerimientos de seguridad y estándares mínimos establecidos por cada Administrador de
Componente en conjunto con el Comité de Seguridad de la Información. En caso que un dispositivo no cuente con los estándares establecidos, éste debe ser desconectado de la red

hasta que sea configurado con los requerimientos definidos. El Comité de Seguridad de la Información realizará revisiones periódicas de las configuraciones y estándares aplicados en los diferentes Componentes Tecnológicos con el fin de evaluar y velar por el cumplimiento de los requerimientos de Seguridad de la Información.

Cualquier ingreso o conexión a las redes corporativas, modem o de acceso remoto por un tercero debe estar aprobada previamente por el Comité de Seguridad de la Información. Un análisis de riesgos debe ser efectuado y los respectivos requerimientos de seguridad deben ser establecidos previamente a la conexión efectuada por el tercero. Todo debe quedar documentado.

11.10.2.40. Papel reciclado y orden en el puesto de trabajo.

Todos los funcionarios deben mantener sus escritorios y áreas de trabajo libres de todo material que contenga cualquier información considerada como confidencial, a menos que esta se esté utilizando por personal autorizado; este deberá garantizar el aseguramiento adecuado de la misma en horarios no laborales y/o ausencia de su puesto de trabajo.

- Aseguramiento de la información confidencial

Toda información impresa y/o en medios magnéticos que no esté siendo utilizada deberá ser asegurada en forma adecuada, usando para esto archivadores, cajas fuertes o muebles destinados para su almacenamiento.

- Fuga de información

Todo funcionario que tenga acceso a información confidencial en medios físicos deberá prevenir la divulgación no autorizada de la misma a personas que trabajen en ambientes o módulos de trabajo cercanos o ajenos a la compañía.

- No reciclaje de papel con información confidencial

Todo documento que contenga información clasificada como confidencial no podrá ser reciclado; deberá ser destruido utilizando medios que impidan la reconstrucción de dicha información.

11.10.2.41. Revisión de Permisos de Acceso Servicios de Red

Los Administradores de cada servicio de Red o quien designe el Rol de Tecnología deben efectuar revisiones trimestrales a los diferentes usuarios que tienen acceso en cada uno de los componentes. Estas revisiones deben incluir como mínimo:

- Usuarios habilitados en los sistemas de Información y que ya no laboren para las Compañías.
- Usuarios con rol de Administración.
- Usuarios que presenten inactividad en la cuenta mayor a 60 días.
- Usuarios genéricos.
- Usuarios que no cumplan con los estándares de creación y complejidad de contraseña.

Las evidencias y soporte de las revisiones deben ser debidamente identificados y documentados; almacenados bajo custodia junto con los documentos relacionados con la revisión. Esta información debe estar disponible para efectos de revisiones y auditorias.

Una vez se efectúe las revisiones cada responsable del Componente Tecnológico debe ajustar los permisos y efectuar las medidas a que dé lugar.

11.10.2.42. Acceso a Recursos en Sistemas de Información

Para cada sistema de Información de las empresas debe existir un dueño o propietario de la información quien debe pertenecer al Rol funcional y debe ser responsable de la administración del módulo de seguridad.

Las Gerencias del negocio deben definir, los esquemas de acceso y los privilegios de usuario para quienes están autorizados a hacer uso de los sistemas de información.

Revisiones trimestrales, se deben efectuar a los perfiles de acceso definidos y matriculados en el aplicativo en producción, determinando las excepciones sobre los siguientes puntos de mayor riesgo:

- Usuarios habilitados en los sistemas de Información y que ya no laboren para la Compañía.
- Cumplimiento con el estándar para la creación de usuarios.
- Revisión de los perfiles de acceso de acuerdo a las actividades propias de cada usuario creado en el sistema de Información.

Las evidencias y soporte de las revisiones deben ser debidamente identificadas, segregadas y bajo custodia, con formularios y documentos relacionados con la revisión de perfiles de usuario. Esta información debe estar disponible para efectos de revisiones de y auditorías.

La sesión en las estaciones de trabajo desde donde se acceden los sistemas de información del negocio, deben tener definido un período de tiempo sin transaccionalidad, después del cual se debe cancelar la sesión. Este tiempo es definido por cada dueño del sistema de Información y debe ser aprobado por el Rol de Tecnología.

Contratistas o terceros que sean autorizados para acceder a los sistemas de información del negocio, estarán restringidos en acceso a datos clasificados como "sensitivos" a la vez que cláusulas de confidencialidad y privacidad registradas en el contrato junto a los respectivos esquemas de penalización por incumplimiento de éstas, se formalizarán para el efecto.

11.10.2.43. Interfases Sistemas Financieros.

Ninguna interfase de usuario final que tenga impacto en el sistema de información financiero deberá estar controlada por personal del Rol de Tecnología. También debe mantener la documentación actualizada del funcionamiento de cada una de las interfaces que tengan impacto financiero.

Cualquier modificación en las interfaces con impacto financiero debe cumplir la política y procedimiento de control de cambios.

Las estructuras de datos con sus características nombre de la variable, longitud y tipo de formato de los archivos que se utilicen en el proceso de interfaces estarán actualizadas y disponibles para consulta en forma permanente.

Ninguna interfase puede ser cargada a los sistemas de Información sin efectuar las validaciones mínimas que garanticen la integridad y consistencia de los datos.

Todas las interfaces deben contar con mecanismos de totales de control que involucren validaciones sobre los campos más críticos.

Todo procesamiento de interfaces debe contar con un registro de inconsistencias.

11.10.2.44. Gestión de Vulnerabilidades en la Plataforma Tecnológica.

Para todos los activos de la plataforma tecnológica que soporta la operación del negocio, se deben ejecutar procedimientos de aseguramiento que garanticen un nivel exigible de disponibilidad, confidencialidad e integridad de la información almacenada, procesada o transportada en cada uno de los activos.

El Comité de Seguridad de la Información definirá las guías de aseguramiento para cada una de las plataformas tecnológicas que soportan la operación del negocio en PLASPEL SAS.

Es responsabilidad de cada una de las áreas encargadas de los activos tecnológicos, aplicar a cada uno de sus activos las guías de aseguramiento definidas previamente.

El Comité de Seguridad de la Información, por medio de un experto tercero contratado, será responsable de ejecutar una vez al año pruebas pasivas de análisis de vulnerabilidades a los activos críticos tecnológicos de PLASPEL SAS.

Es responsabilidad de cada una de las áreas encargadas de los activos tecnológicos, solicitar al Rol corporativa de seguridad de la información la ejecución de pruebas pasivas de análisis de vulnerabilidades en sus activos cada vez que se realice un cambio total o una modificación crítica en el activo. Estas pruebas entraran en el cronograma anual de análisis. Se entiende como modificación crítica: cambio o reinstalación del sistema operacional del activo, cambios en las políticas de seguridad del activo, cambio de un componente físico de procesamiento de información del activo.

Es responsabilidad de cada una de las áreas encargadas de los activos tecnológicos, ejecutar las acciones pertinentes que mitiguen los riesgos ocasionados por las amenazas detectadas en el análisis de vulnerabilidades.

Es responsabilidad de las áreas encargadas de los activos tecnológicos mantener un nivel bajo o aceptable de riesgo en los activos.

El Rol corporativa de seguridad de la información reportará periódicamente a la gerencia de tecnología
Informática el estado del indicador de aseguramiento de la plataforma tecnológica.

11.10.2.45. Sincronización de relojes.

Los relojes de los sistemas dentro de PLASPEL SAS deben estar sincronizados con un tiempo acordado. Debe establecerse según una norma aceptada mitigando el riesgo de fallas en la información por diferentes horas de los sistemas.

11.11. GESTIÓN DE SEGURIDAD PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION

11.11.1. Política de Adquisición, Desarrollo y Mantenimiento de sistemas

El Rol de Tecnología debe proveer medidas de seguridad en sistemas de información desde la fase de requerimientos, y deben ser incorporados en las etapas de desarrollo, implementación y mantenimiento. 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

Todos los sistemas de información o desarrollos de software deben tener un Rol propietaria

Las áreas propietarias de los sistemas de información, en acompañamiento con el Comité de Seguridad de la Información deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la 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.

Los desarrolladores 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. 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 el Rol de Tecnología 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.

11.11.2 Estándares de la Política de Adquisición, Desarrollo y Mantenimiento de Sistemas

11.11.2.1. Requerimientos de seguridad de los sistemas.

El Rol de Tecnología debe asegurar que todas las actividades relacionadas con el desarrollo y mantenimiento de sistemas de información, consideren la administración de los riesgos de seguridad. Todos los requerimientos de seguridad se deben identificar durante la etapa de requerimientos, al igual que justificar, acordar y documentarse, como parte de todo el proyecto del sistema de información.

11.11.2.2. Seguridad de las aplicaciones del sistema.

Se deben desarrollar estándares que indiquen cómo se deben asegurar los diferentes sistemas, aplicaciones y desarrollos, para minimizar la aparición de errores, pérdidas y modificaciones no autorizadas o usos indebidos en la información de las aplicaciones. Se deben diseñar controles adecuados en las aplicaciones, para garantizar un correcto procesamiento. Se debe incluir la validación de los datos introducidos, el procesamiento interno y los datos resultantes. Las aplicaciones que se desarrollen en PLASPEL SAS deben cumplir unos requerimientos mínimos de seguridad, conforme a las buenas prácticas en seguridad de la información y a esta política de seguridad. El diseño y operación de los sistemas debe obedecer a estándares de seguridad comúnmente aceptados y la normatividad vigente.

11.11.2.3. Seguridad de los sistemas de archivos.

Se debe controlar el acceso al sistema de archivos y al código fuente de los programas. La actualización del software aplicativo, las aplicaciones y las librerías, sólo debe ser llevada a cabo por los administradores.

11.11.2.4. Seguridad de los procesos de desarrollo y soporte.

Se requiere de un control estricto en la implementación de cambios. Los procedimientos de control de cambios deben validar que los procesos de seguridad y control no estén comprometidos; igualmente deben cerciorarse de que los programadores de apoyo posean acceso sólo a las partes en el sistema necesarias para desarrollar su trabajo, que dichos cambios sean aprobados con un procedimiento adecuado y con la documentación correspondiente.

Los 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.

El Rol de Tecnología 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. 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. 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 del instituto.

El Comité de Seguridad de la Información 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.

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; 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 o 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.

11.12. CUMPLIMIENTO Y NORMATIVIDAD LEGAL

11.12.1. Política para el Cumplimiento y Normatividad Legal

Toda solución de servicios o infraestructura tecnológica debe garantizar que su selección está de acuerdo con las condiciones contractuales, de legislación y regulación externa e interna, para el debido cumplimiento de los regímenes legales a los cuales está sometida la organización.

11.12.2. Estándares de la Política para el Cumplimiento y Normatividad Legal

11.12.2.1. Cumplimiento legal.

Todos los requerimientos contractuales y legales que puedan afectar los sistemas de información de PLASPEL SAS, deben definirse previamente y documentarse de acuerdo con la metodología empleada por la empresa. Los controles específicos, medidas de protección y responsabilidades individuales que cumplan con los requerimientos, deben así mismo definirse y documentarse. El Rol jurídica de PLASPEL SAS asesorará al Comité de Seguridad en dichos aspectos legales específicos.

Las políticas de seguridad de información de PLASPEL SAS fueron diseñadas para ajustarse o exceder, sin contravenir, las medidas de protección establecidas en las leyes y regulaciones, si algún funcionario y/o tercero de PLASPEL SAS considera que alguna política de seguridad de información está en conflicto con las leyes y regulaciones existentes, tiene la responsabilidad de reportar en forma inmediata dicha situación al Comité de Seguridad de la Información, quien atenderá la situación.

4.12.2.2. Propiedad intelectual.

Se protegerá adecuadamente la propiedad intelectual de PLASPEL SAS, tanto propia como la de terceros (derechos de autor de software o documentos, derechos de diseño, marcas registradas, patentes, licencias, código fuente, entre otros). El material registrado con derechos de autor no se debe copiar sin la autorización del propietario.

11.12.2.3. Protección de datos.

Los estándares de seguridad son de obligatorio cumplimiento para los funcionarios con acceso a los datos de carácter personal y a los sistemas de información. Deberán considerar, los siguientes aspectos:

- Ámbito de aplicación del procedimiento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido por la ley.
- Funciones y obligaciones del personal con acceso a las bases de datos.
- Estructura de las bases de datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante los incidentes.
- Procedimientos de realización de copias de respaldo y de recuperación de los datos.
- Controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el procedimiento de seguridad que se implemente.
- Medidas a adoptar cuando un soporte o documento va a ser transportado, desechado o reutilizado. El procedimiento se mantendrá actualizado en todo momento y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

11.12.2.4. Cumplimiento de políticas y normas de seguridad.

Los directivos de la compañía se deben asegurar que todos los procedimientos de seguridad dentro de su Rol de responsabilidad se realizan correctamente, con el fin de cumplir las políticas y normas de seguridad; en caso de incumplimiento se evaluaran y propondrán acciones correctivas. Los resultados de estas revisiones serán mantenidos para su revisión con auditoria.

11.12.2.5. Cumplimiento técnico.

Se debe comprobar periódicamente que los sistemas de información cumplen con las normas de implementación de seguridad. Se deben realizar auditorías periódicas con ayuda de herramientas automatizadas y se deben generar informes técnicos que reflejen la evaluación de riesgos de seguridad de la información, las vulnerabilidades y su grado de exposición al riesgo.

12. DOCUMENTACIÓN RELACIONADA

En apoyo a los principios de Seguridad de la Información, apoya en contexto:

- Código de Buen Gobierno Corporativo.
- Sistema de Gestión de la Calidad y Política Ambiental de la organización.
- Política de Gestión Humana.
- Política de tecnología de información y comunicación.

13. POLÍTICA DE PRIVACIDAD Y PROTECCION DE DATOS PERSONALES

En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, PLASPEL SAS, propenderá por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información. Se establecerán los términos, condiciones y finalidades para las cuales la entidad, 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 el instituto, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, la Compañía 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 funcionarios, estableciendo los controles necesarios para preservar aquella información que el instituto conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias del instituto y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

Las Áreas que tienen contacto con datos personales 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 Compañía. 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.

El Comité de Seguridad de la Información debe establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, proveedores y demás terceros de los cuales reciban y administre información.

El Rol de Tecnología debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, 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.

Los funcionarios directos o indirectos deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información del instituto o de sus funcionarios 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.

Los usuarios de las aplicaciones para clientes de PLASPEL SAS 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. Deben aceptar el suministro de datos personales que pueda hacer el instituto 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.

14. ROLES Y RESPONSABILIDADES

15.1. COMPROMISO DE LA DIRECCION

El Consejo de Administración de PLASPEL SAS 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. El Consejo de Administración y la Alta Dirección de la entidad demuestran 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 funcionarios de la entidad.
- 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

15.2. COMITÉ DE SEGURIDAD DE LA INFORMACION

- El Comité de Seguridad de la Información está conformada por el responsable del Rol de Tecnología –que lo preside - y por el responsable del Rol de Riesgos y Control Interno, junto con las personas previamente solicitadas de forma eventual.
- Debe actualizar y presentar ante el Consejo de Administración las Políticas de Seguridad de la Información, la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.
- El Comité de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.
- El Comité de Seguridad de la Información debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.

15.3. ROL DE TECNOLOGIA

- La Oficina de Tecnología debe liderar la generación de lineamientos para gestionar la seguridad de la información de PLASPEL SAS y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.
- La Oficina de Riesgos debe validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.

15.4. AUDITOR

- Debe planear y ejecutar las auditorías internas al Sistema de Gestión de Seguridad de la Información de PLASPEL SAS a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.
- Debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.
- Debe informar a las áreas responsables los hallazgos de las auditorías.

15.5. TODOS LOS FUNCIONARIOS DE PLASPEL SAS

- Cumplimiento íntegro por rol, acción u omisión del presente documento y adicionales.
- Todos los colaboradores actuarán con las mediciones periódicas que hará el Consultor elegido para tal fin en adelante, para certificar el cumplimiento de este Sistema de Administración de Riesgo.

16. POLÍTICA DE PRIVACIDAD Y PROTECCION DE DATOS PERSONALES

En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, PLASPEL SAS a través del Rol de Riesgos, propenderá por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información. Se establecerán los términos, condiciones y finalidades para las cuales PLASPEL SAS, 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 Entidad, hayan suministrado datos personales.

En caso de delegar a un tercero el tratamiento de datos personales, PLASPEL SAS 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 funcionarios, estableciendo los controles necesarios para preservar aquella información que la Entidad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias del negocio y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

16.1. Normas de privacidad y protección de datos personales.

- Las áreas que procesan datos personales de beneficiarios, funcionarios, 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 Entidad.
- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.
- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.

- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes 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.
- Las áreas que procesan datos personales de beneficiarios, proveedores u otras terceras partes 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
- Los usuarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de PLASPEL SAS, o de sus funcionarios 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.

ANEXO 1. ACUERDO SEGURIDAD DE LA INFORMACION

ACUERDO DE RESPONSABILIDAD EN SEGURIDAD DE LA INFORMACIÓN PARA STAKEHOLDERS DE PLASPEL SAS

Yo, _____, identificado con ___ No. _____, en calidad de representante legal de _____ con NIT, o en nombre propio __, en virtud de la relación con PLASPEL SAS como _____, recibo de forma íntegra, en concordancia con las normas de Seguridad de la Información competentes, la responsabilidad del buen uso de la información física o digital

derivada de mi relación con PLASPEL SAS, por lo que suscribo el presente Acuerdo de responsabilidad en seguridad de la información, por el que declaro conocer y aceptar que:

- Me hago responsable de no divulgar, revelar ni alterar mi clave personal, la información confidencial, procedimientos, formatos, y demás aspectos técnicos y administrativos que se generen dentro del sistema, derivados de la entrega del usuario y clave de la institución, para proteger la información contra uso desautorizado o incorrecto, aún después que haya terminado mi relación laboral con la Institución a la cual me pertenezco.
- La clave es un mecanismo importante para la protección de los sistemas y aplicaciones. Por lo cual entiendo que su manejo es personal e intransferible. Y acuerdo no divulgar la(s) clave(s) de acceso a mí, asignadas a ninguna persona.
- Entiendo que el usuario que me asignen y clave, son exclusivamente para mi uso y para propósitos de trabajo. Y estoy consciente que cualquier actividad en los sistemas, haciendo mal uso de mis claves es de mi responsabilidad.
- Es mi responsabilidad informarme, entender, apoyar y cumplir con las normas de seguridad que gobiernan la protección de los activos de la información
- En caso de pérdida, olvido o sustracción del Identificador de Usuario y clave de acceso, me obligo a comunicar con las personas responsables de la entidad respectiva, de manera inmediata
- Seré responsable de las consecuencias administrativas, civiles y penales establecidas en la Ley, por la pérdida, olvido o sustracción del Identificador de Usuario y clave de acceso, así como por las que se deriven del uso indebido de la información.
- Seré responsable de entregar mediante acta de entrega recepción el identificador de usuario y clave de acceso al momento de mi cese de funciones, vacaciones, comisiones y ausencias temporales a la institución con la finalidad de que estas se deshabiliten en el sistema.
- Reconozco que soy responsable por el uso de mi Identificador de Usuario y clave de acceso, de producirse o presumirse la pérdida olvido o sustracción hasta el momento en que sea notificado mediante comunicación escrita (correo electrónico, oficio) a la Institución.
- Acuerdo poner en conocimiento de la autoridad según corresponda, inmediatamente, cualquier comportamiento o situación sospechosa que puedan poner en peligro los activos de información en el sistema de administración de las finanzas públicas
- Entiendo que PLASPEL SAS puede revisar cualquier información que yo haya generado. Estoy consciente que se harán auditorías periódicas del manejo que yo haga de la información.
- Es de mi responsabilidad dar cumplimiento a las recomendaciones de seguridad de la información solicitadas por PLASPEL SAS
- Debo cumplir con los procedimientos de borrado seguro, demostrándolo a PLASPLE SAS

- En general debo cumplir con las normas ISO 27001, Circulares Externas de la Superintendencia Financiera 052 de 2011, 052 de 2007, 042 de 2012; Ley 527-1999 Ley de comercio electrónico, y derivadas de las anteriores., cuando gestione cualquier tipo de información de PLASPEL SAS, so pena de las medidas legales y comerciales que la omisión de este punto implique.

En constancia de haber leído y acatado lo anterior firmo el presente documento a los_____ días del mes de _____ de _____ en la ciudad de _____.

FIRMA DEL CLIENTE_____

NOMBRE_____

C.C _____ **Huella Índice Derecho**

REPRESENTANTE LEGAL DE_____NIT _____

ANEXO 2. CUMPLIMIENTO TERCEROS SEGURIDAD DE LA INFORMACION

Documento aparte, integral a este documento

CONTROL DE CAMBIOS

CONTROL DE CAMBIOS			
23-05-22	v1	**INCLUSION**	Creación del Documento
		MODIFICACION	NA
		EXCLUSION	NA