POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

TABLA DE CONTENIDO

1 POLÍTICAS DE SEGURIDAD DE INFORMACIÓN Y CIBERSEGURIDAD

Para POWERDATA la seguridad de la información de sus pymes así como de sus clientes personas naturales y/o jurídicas, y otros usuarios, resulta fundamental proteger, además garantizar los activos que la contienen, de cualquier pérdida de confidencialidad, integridad o disponibilidad, tanto accidental como intencionada; teniendo en cuenta la normatividad, cumpliendo la Modelo de Seguridad y Privacidad de la Información – MSPI del gobierno colombiano y demás regulaciones aplicables, todo esto mediante la implementación de medidas apropiadas relacionadas con: la ciberseguridad, las personas, los procesos, la tecnología, la infraestructura y los servicios relacionados con analítica de datos en Pymes; y a través del fortalecimiento de la confianza que nos caracteriza la relación con nuestros clientes, miembros y usuarios.

1.1 ALCANCE

La política de seguridad de la información aplica, pero no se limita, a:

- La información de clientes, comercios y el software de analítica de datos.
- La información generada como resultado de la operación y prestación de los servicios.
- Todos los activos de información de Powerdata a través de su ciclo de vida, incluyendo creación, distribución, almacenamiento y disposición final, priorizando su protección acorde con las evaluaciones de riesgos. .
- Todos los activos de información de las entidades asociadas en cuyo ciclo de vida Powerdata intervenga incluyendo creación, distribución, almacenamiento y disponibilidad según corresponda.
- Todos los ambientes de procesamiento de información (producción, desarrollo y pruebas, entre otros)
- Todos los colaboradores, aliados, contratistas y terceros que usen, tengan acceso o sean responsables de la información y todo el personal que diseñe, opere o sea responsable por sistemas manuales y computarizados que contengan información de Powerdata debe cumplir con estas políticas.

1.2 ACTUALIZACIÓN

La Dirección de Seguridad de la Información es la responsable del mantenimiento y la revisión continua de estas políticas, cuyos cambios deben ser presentados al Comité de Presidencia y/o Comité de Procesos y Riesgos de la organización y compartidos a sus respectivos participantes para que en un transcurso de ocho (8) días hábiles se

reciban comentarios y así proceder con los ajustes necesarios. Si no se reciben comentarios, automáticamente se aprobará la actualización de las Políticas de Seguridad de la Información y Ciberseguridad. Posteriormente, las Políticas de Seguridad de la Información son divulgadas en el Sistema de Gestión de Calidad de Powerdata e informadas vía correo electrónico a todos los colaboradores y terceros críticos de Powerdata.

Esta revisión se debe llevar a cabo mínimo una vez al año o en respuesta a cualquier cambio que pueda afectar la seguridad de los datos de la organización, (p.ej. incidentes de seguridad de la información, nuevas vulnerabilidades, actualizaciones de estándares de industria y/o legislación colombiana, entre otros).

2 ORGANIZACIÓN DE SEGURIDAD

Directivas y lineamientos para la gestión de la Seguridad de la Información y ciberseguridad en Powerdata.

2.1 GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Powerdata establece mecanismos para asegurar la implementación y gestión de los lineamientos establecidos en las normas relativas a la seguridad de la información y ciberseguridad establecidas por la Superintendencia Financiera de Colombia y estándares internacionales como ISO 27001 y DBMS. Además, garantiza la designación de personal experto encargado de la gestión de la información, dirigiendo de esta forma, las actividades de mantenimiento y mejora de la seguridad de la información y ciberseguridad de manera continua.

La estructura de gestión de la seguridad de la información se encuentra descrita en el Manual de Sistema de Gestión de Seguridad de la Información.

3 GESTIÓN DE ACTIVOS DE INFORMACIÓN

Directivas para mantener la protección adecuada de los activos de información.

3.1 INVENTARIO DE ACTIVOS DE INFORMACIÓN

Powerdata debe mantener, por cada una de las categorías de activos de información, un inventario de activos de infraestructura de TI, aplicaciones, personas, proveedores y activos físicos que soportan las operaciones básicas y críticas de la compañía. Dichos inventarios consideran aspectos como datos técnicos, identificación del activo,

responsable técnico, responsable de la aplicación, dueño de la información, descripción del activo y ubicación física entre otros. La actualización de la información registrada en el inventario para cada uno de los tipos de activos de información debe realizarse mínimo una vez al año o cuando se presenten cambios con impacto alto en la plataforma de Powerdata; igualmente, para cada activo se debe identificar si pertenece al de gestión de bases de datos o no está relacionado con este tipo de dato confidencial.

Las categorías de activos de información en Powerdata y los responsables de su gestión son:

CATEGORIAS	DESCRIPCION	RESPONSABLE
Información	Listado Maestro de Documentos y Listado Maestro de Registros	Dirección de Procesos
Infraestructura de TI	Inventario de Infraestructura de TI	Administradores de plataformas
Aplicaciones/Software	Inventario de aplicaciones	Administradores de aplicaciones
Personas	Listado de Cargos Críticos	Gerencia de Talento Humano
Servicios contratados / outsourcing	Listado de contratos críticos	Direccion de Servicios Administrativos
Activos físicos	Mobiliario donde se almacene información impresa (escritorios, bibliotecas, archivadores, etc.)	Dirección de Servicios Administrativos

3.2 SOFTWARE AUTORIZADO

En Powerdata solo se permite la utilización de software legal y debidamente licenciado, para esto, debe existir un control y registro del software autorizado, entre lo que se encuentra, pero no se limita a:

- Herramientas de ofimática
- Utilitarios
- Herramientas para administración de sistemas de información
- Herramientas para borrado seguro
- Herramientas para desarrollo
- Entre otros.

Incidentalmente es permitido utilizar software de código abierto (Free, OpenSource), previa evaluación por parte de Seguridad de la Información en conjunto con la Dirección de TI&TELCO y solo para las actividades debidamente justificadas de negocio.

Utilizar software ilegal y/o no autorizado se considera un incumplimiento a las políticas internas de Powerdata, regulaciones aplicables y de ley, por lo tanto, se debe aplicar los controles necesarios para evitar la instalación de software no controlado y eliminar cualquier posibilidad de mal uso a través de aplicaciones con fines indebidos.

3.3 CLASIFICACIÓN DE INFORMACIÓN

Powerdata debe proteger la integridad, confidencialidad y disponibilidad de la información corporativa con el debido cuidado de acuerdo con su nivel de clasificación. Esa información incluye, pero no está limitada a: reportes, presentaciones, correos electrónicos, memorandos, u otro material creado por personas y usado para llevar a cabo actividades del negocio o para soportar decisiones gerenciales.

Toda la documentación de Powerdata debe contar con la debida clasificación de la información tal y como lo establece el instructivo de Clasificación, Etiquetado y Protección de la Información (CIS104-IN04).

3.4 USO PERSONAL DE LOS SISTEMAS Y ACTIVOS DE INFORMACIÓN DE POWERDATA

El uso de los sistemas y activos de información de Powerdata están destinados únicamente para propósitos de negocio. Incidentalmente el uso personal es permisible si dicho uso:

- No viola ninguna política establecida.
- No viola la legislación vigente.
- No consume más que un monto insignificante de los recursos que podrían ser utilizados para fines del negocio.
- No interfiere con la productividad del colaborador que lo usa o de otros colaboradores.
- No prima sobre ninguna actividad del negocio.
- No afecta la disponibilidad de la información o los servicios prestados por POWERDATA.

3.5 USO DE DISPOSITIVOS ELECTRONICOS PERSONALES

No se permite la utilización de dispositivos personales (portátiles, tablets, smartphones, medios extraíbles, entre otros) para ejecutar las actividades laborales, acceder a la red, los servicios ni aplicaciones de Powerdata. Incidentalmente se permite utilizarlos dentro de las instalaciones de Powerdata siempre y cuando el uso de estos no intervenga con la productividad y el desempeño de las funciones de cada colaborador. Es responsabilidad de los respectivos jefes inmediatos velar por un uso adecuado de dichos dispositivos.

3.6 USO DE DISPOSITIVOS ELECTRÓNICOS CORPORATIVOS

Powerdata podrá otorgar dispositivos electrónicos corporativos (como laptops, smartphones y medios de almacenamiento extraíbles) a sus colaboradores siempre y cuando exista una justificación de negocio y/o un concepto de Seguridad de la Información. El uso de estos dispositivos es 100% corporativo y Powerdata podrá auditar los mismos cuando lo disponga. Los colaboradores y/o terceros con dispositivos electrónicos corporativos están sujetos a:

- No instalar software no autorizado sin previa justificación o concepto por parte de Seguridad de la Información.
- No hacer uso de los dispositivos electrónicos corporativos para fines personales.
- Velar por la protección y seguridad de dichos dispositivos.
- Autenticarse mediante un ID y contraseña asignada por Powerdata.

La descripción para la configuración de equipos de acuerdo con las políticas establecidas en este documento se encuentra descrita en el instructivo “Estándar de Configuración Segura de PC’s”, STC134-AN009.

El proceso para la autorización, entrega e instalación de dispositivos se encuentra descrito en el procedimiento “Gestión de Dispositivos Tecnológicos Usuarios”, STC124.

3.7 USO INADECUADO DE LOS SISTEMAS Y ACTIVOS DE INFORMACIÓN DE POWERDATA

Los colaboradores de Powerdata deben usar los sistemas y activos de información como parte de las funciones de su trabajo y/o en beneficio de Powerdata, excepto en los casos que define la política de uso personal de sistemas y activos de información. Los colaboradores no deben dar uso inadecuado a los sistemas y activos de información de tal forma que pueda generarse intencionalmente o no, un impacto negativo sobre el negocio o que ponga en riesgo los procesos de Powerdata.

3.8 USO DEL CORREO ELECTRÓNICO

El servicio de correo electrónico dispuesto por Powerdata se constituye en un medio a través del cual los colaboradores de Powerdata, las entidades miembros, los proveedores y demás agentes externos que de una u otra manera se vinculan con la operación de Powerdata, pueden comunicarse dentro y fuera de la organización para fines relacionados con el negocio y no debe ser objeto de abusos.

Con base en la normatividad legal vigente aplicable al sector financiero, No se permite el envío o recepción de correos electrónicos, la mensajería instantánea, ni ningún otro servicio que permita el intercambio de información en los equipos de cómputo usados en las áreas con acceso a información CONFIDENCIAL. Dependiendo de las necesidades del negocio, se podrá otorgar permisos para el envío y/o recepción de correos electrónicos a dichas áreas, con previa autorización y justificación de negocio, siempre y cuando Powerdata cuente con un sistema de registro de la información enviada y recibida. Dicho sistema de registro de información enviada y recibida será monitoreado permanentemente para garantizar que no hay fuga de información sensible ni recepción de información que pueda comprometer la seguridad de la organización.

El servicio de correo electrónico puede ser utilizado por terceros permanentes previa solicitud del funcionario encargado del tercero y aprobación por su jefe inmediato y por la Gerencia de Infraestructura y Telecomunicaciones.

3.8.1 INTERCAMBIO DE INFORMACION CONFIDENCIAL A TRAVES DE CORREO ELECTRONICO CORPORATIVO

No se debe intercambiar información confidencial a través de correo electrónico corporativo. Si por necesidad del negocio es requerido, esto debe realizarse de forma segura, utilizando algoritmos de cifrado fuerte. Dependiendo del mecanismo que se utilice para el cifrado de la información, se debe garantizar que la contraseña para descifrado no se transmita por el mismo medio y cumpla con las políticas definidas en el procedimiento de Gestión de Usuarios (TEC134).

Para los casos en que se recibe la información por parte de clientes, comercios y/o terceros, se debe realizar debida diligencia comunicando que todo dato de tarjeta enviado debe ser cifrado bajo algoritmos de cifrado fuertes; así mismo, se debe asignar una contraseña fuerte de acceso al archivo ".pst" donde se almacenan estos correos.
Los correos recibidos pueden tener un tiempo de retención hasta por 5 años, una vez cumplido este periodo de tiempo, se debe realizar borrado seguro en el equipo y realizar almacenamiento en el File Server Seguro o disposición final definida por cada área.

Las áreas de Powerdata que en sus funciones gestionen usuarios de analítica de datos con POWER BI como la Dirección operativa, dirección administrativa y las mismas

Pymes además de los stakeholders, solo tienen permitido el envío de correos externos a los gerentes de área dentro de la organización para validar la gestión de la información.

3.8.2 SERVICIO CORREO ELECTRONICO CORPORATIVO FUERA DE LA RED DE POWERDATA

El acceso al servicio de correo electrónico corporativo fuera de las instalaciones de Powerdata está restringido, razón por la que el acceso a correo electrónico fuera de las instalaciones de Powerdata está dispuesto exclusivamente para uso de los Coordinadores, directores, Gerentes, Vicepresidentes y Presidente, a través de los equipos portátiles de la compañía mediante la habilitación del servicio RPC por HTTP conocido como Outlook Anywhere. Con esta tecnología, se podrá consultar el correo electrónico a través de internet mediante el cliente tradicional de Outlook y únicamente desde los equipos portátiles de Powerdata.

Cuando por necesidad del negocio, se requiere habilitar este servicio a colaboradores de otros cargos, se debe generar un concepto de Seguridad de la Información donde se identifiquen los riesgos asociados a la necesidad y los respectivos controles de seguridad que eviten posibles incidentes de fuga de información u algún otro riesgo que aplique.

3.9 USO DEL INTERNET

El acceso a Internet debe ser aprobado, manejado con seguridad y usado principalmente para fines relacionados con las actividades laborales.

- No se permite la navegación por Internet en los equipos de cómputo usados en áreas con acceso a información confidencial, u otra aplicable tales como: Contact Center, la Unidad de Monitoreo, los asignados a los Analistas de Medios de Acceso y a los Operadores del Centro de Computo, así como los asignados para la generación e inyección de llaves MK de POS, a menos que se asignen accesos específicos de navegación de acuerdo con la necesidad del rol previa autorización según procedimiento de Gestión de Usuarios, en ningún caso se podrán asignar accesos que permitan la consulta de correos electrónicos personales.

- Por definición de la organización, se permite el acceso eventual a redes sociales de forma temporal para participar en campañas a través de estos medios, siempre y cuando no afecte las actividades laborales normales ni incumpla las demás políticas de seguridad de la información, estándares y regulaciones aplicables. Esto debe hacerse de forma controlada de tal manera que se evite posibles incidentes de seguridad de la información.

- A continuación, se establecen los lineamientos en relación con el uso de internet:

.

  - Powerdata se reserva el derecho de realizar supervisión de los sitios de Internet visitados y del uso de los servicios habilitados.

  - Está estrictamente prohibido acceder a sitios Web o la utilización de programas para la descarga de videos y/o música.

  - Se prohíbe representar a la compañía en nuevos grupos, redes sociales o en otros foros públicos a menos que previamente sea autorizado.

  - Los colaboradores de Powerdata deben asegurarse de no acceder a información recibida vía Internet que no provenga de fuentes conocidas y confiables.

  - Los colaboradores no deben publicar información de Powerdata como descripción de sistemas, software, comunicados. internos, bases de datos, o cualquier tipo de información confidencial en cualquier sistema de acceso público como Internet, a menos que esto haya sido aprobado al interior de Powerdata.

  - El uso de aplicaciones de mensajería instantánea pública y/o p2p (peer to peer) (ej AIM, Yahoo Messenger, Skype, Ares, Emule, entre otros) está prohibido. La Información confidencial no debe ser transmitida a través de Internet sin el debido cifrado fuerte que garantice la protección de su confidencialidad.

  - No se permite realizar descargas a través de internet. Los colaboradores de Powerdata deben abstenerse de visitar o descargar información o programas de sitios que no estén aprobados. Se consideran sitios inapropiados aquellos que proveen información o métodos para violar los controles normales de seguridad (ej sitios de hackers), contienen software ilegal o no licenciado, o que relacionan con juegos en línea o que puedan describirse como de contenido sexual explicito, de discriminación por razones de raza, color, sexo, orientación sexual, credo o religión.

  - Está prohibido acceder a sitios de almacenamiento en la nube (p. ej. Google Docs, skydrive, OneDrive, Dropbox, Google Drive, entre otros). Por necesidad de negocio y con previa justificación por parte de cargos directivos, el acceso a estos sitios web podría otorgarse a colaboradores en específico, teniendo en cuenta el concepto emitido por el área de Seguridad de la

Información y la implementación de los controles que permitan asegurar de forma adecuada la información catalogada como confidencial en Powerdata.

- Para todo colaborador, aliado, contratista y tercero que tenga acceso al dominio de Powerdata, está prohibido el ingreso a cuentas de correo electrónico personales (p. ej. Gmail, Hotmail, MSN, Yahoo, Outlook, etc).

- Los colaboradores de Powerdata no deben establecer contratos de conexión con proveedores de Internet o redes externas sin cumplir los procedimientos establecidos y las debidas aprobaciones.

- Todo software y/o archivo descargado de origen externos debe ser verificado con un antivirus dispuesto por la Dirección de TI&TELCO.

- Para los colaboradores que cuenta con equipos portátiles y dispositivos móviles asignados por Powerdata, deben:

    a. No utilizar redes de acceso a internet no confiables para transmitir información confidencial y/o de uso interno.
    b. Compartir el acceso a internet externo (operador, wifi externa) con los equipos de la red interna.
    c. Abstenerse de utilizar al mismo tiempo la conexión a la red interna de Powerdata y el acceso a una red externa.

Cualquier excepción de acceso a Internet diferente a lo establecido en las Políticas debe ser enviada a la Dirección de Seguridad de la Información para la emisión de un concepto y su respectiva aprobación.

4 SEGURIDAD DEL TALENTO HUMANO

Lineamientos y estrategias para reducir los riesgos relacionados con los colaboradores.

4.1 ROLES Y RESPONSABILIDADES

Los roles y responsabilidades de seguridad se encuentran definidos dentro del manual de funciones y perfiles para todos los cargos tanto directos como temporales y contratistas, comunicadas a todo el personal y en constancia de aceptación se deben incluir dentro de los contratos de trabajo la aceptación de estos.

4.2 SELECCIÓN DE PERSONAL

Los posibles colaboradores de Powerdata se deben someter a una pre-selección de acuerdo a la normatividad laboral vigente, a las regulaciones aplicables y las mejores prácticas. Los lineamientos para la selección y contratación del personal de Powerdata están descritos en el procedimiento Selección de Personal (GTH189).

En adición se debe asegurar que el personal de terceras partes a quienes se les ha permitido el acceso regular a las instalaciones de Powerdata, sistemas o a información con clasificación de confidencialidad, son seleccionados de acuerdo con la normatividad laboral vigente, a las regulaciones aplicables y las mejores prácticas. Para estos casos, contractualmente deben especificarse las responsabilidades de las terceras partes frente a la contratación y/o asignación de personal idóneo encargado de prestar sus servicios profesionales a Powerdata.

4.3 CAPACITACIÓN EN SEGURIDAD DE INFORMACIÓN Y CIBERSEGURIDAD

La Dirección de Seguridad de la Información debe contemplar dentro de su programa, aspectos de concientización, capacitación y entrenamiento especializado en seguridad de información y ciberseguridad. Los colaboradores deben recibir capacitación por lo menos una vez al año.

Es responsabilidad del personal directivo de Powerdata asegurar que los colaboradores a cargo (incluyendo contratistas, asesores y/o temporales con acceso a los sistemas de información) participen de los programas de formación y generación de: conciencia en seguridad de información y ciberseguridad, capacitación en las políticas de seguridad de la información y ciberseguridad, su responsabilidad en el manejo de información y en el correcto uso de los recursos.

4.4 PROCEDIMIENTOS PARA EL RETIRO DE COLABORADORES

Powerdata tiene definido dentro de sus procedimientos de gestión del recurso humano, la administración de renuncias voluntarias y terminación involuntaria que permita recuperar los bienes de Powerdata, proteger al personal, los sistemas, la información, aplicaciones y redes (con énfasis en la des habilitación de claves o derechos de acceso a los sistemas de información en especial los que tienen privilegio administrativos y/o acceso remoto) de cualquier riesgo relacionado con personas externas que pueden poseer un conocimiento interno de las operaciones de Powerdata.

Cuando se recoja el equipo de cómputo del colaborador retirado, se debe realizar una copia de la información almacenada en un medio removible de forma segura, realizar borrado seguro del medio de almacenamiento, hacer la entrega al jefe directo y efectuar el registro en la bitácora respectiva.

5 SEGURIDAD FISICA Y DEL ENTORNO

Powerdata ha establecido estrategias para el control del acceso físico a sus instalaciones y el cuidado de los equipos y/o recursos de procesamiento de datos disponibles en la organización. El principal objetivo de estas estrategias es mitigar riesgos potenciales relacionados con la pérdida, el robo o el daño accidental o intencional de los activos de información de la empresa, evitando la interrupción, total o parcial, de las actividades del negocio. Así mismo definir las directivas para la protección física de las instalaciones donde están situados este tipo de recursos.

5.1 CONTROL DE ACCESO FÍSICO

La seguridad física para las instalaciones de Powerdata está basada en la implementación de controles ambientales, sistemas de seguridad electrónicos, personal de seguridad designado, políticas de control de acceso, estándares y procedimientos para asegurar apropiadamente el personal y los activos en las diferentes instalaciones de la compañía.

Las directrices para el control de acceso físico se encuentran descritas en el procedimiento Control de Acceso Físico (GIS82).

5.2 IDENTIFICACIÓN DE COLABORADORES Y VISITANTES

Una vez la pyme Powerdata adquiera sus infraestructura fisica, todos los colaboradores y visitantes que ingresen a sus instalaciones deberán portar un carnet de identificación, asignado específicamente a la persona, de uso personal e intransferible y que debe ser visible, en todo momento, mientras se mantenga en las instalaciones.

5.3 SEGURIDAD EN OFICINAS Y AREAS DE TRABAJO

Es responsabilidad de cada colaborador de Powerdata garantizar que toda la información confidencial de la compañía que mantenga en su poder ya sea en medio físico o electrónico, sea almacenada y protegida del acceso no autorizado.

5.4 PROTECCIÓN FÍSICA DE ACTIVOS

Los colaboradores de Powerdata, deben actuar con la debida diligencia en la custodia, cuidado y buen uso sobre los activos que se les han asignado con el fin de prevenir pérdidas ocasionadas por, daño, acceso no autorizado y amenazas del medio que afecten el activo.

La extracción de equipos de cómputo y de equipamiento de redes de las instalaciones de Powerdata debe ser aprobada y documentada de acuerdo con el procedimiento de Control de Acceso Físico (GIS82).

Todo equipamiento debe ser protegido adecuadamente y salvaguardado para prevenir robo, pérdida y daño cuando es extraído de su ubicación.

5.5 AREAS RESTRINGIDAS O DE PROCESAMIENTO DE INFORMACIÓN CONFIDENCIAL

Los centros de cómputo y zonas definidas como áreas de procesamiento de información confidencial requieren un mayor nivel de exigencia en los controles de acceso y la seguridad física en general, que las demás instalaciones de Powerdata, entre los cuales se encuentran;

a) Sistemas de control de acceso fuerte,
b) UPS para el suministro controlado de energía eléctrica, extintores, control de temperatura y limpieza.
c) Los elementos constructivos internos (puertas, paredes, suelos, etc.) deben cumplir el mínimo nivel de protección exigido por las normas básicas de edificación.
d) Deben disponer de canalizaciones adecuadas para la conducción del cableado de comunicaciones y electricidad, para evitar ataques (sabotaje, fuego, roedores), interceptación o perturbaciones por fuentes de emisión próximas (radio, eléctricas, calor, etc).

6 GESTION DE LAS COMUNICACIONES Y LAS OPERACIONES

Directivas para asegurar la operación de los sistemas de información.

6.1 DOCUMENTACIÓN

Los administradores de telecomunicaciones y sistemas en POWERDATA, deben mantener procedimientos documentados, actualizados y disponibles para quienes lo requieran según los lineamientos establecidos para estos casos en el Sistema de Gestión de Calidad.

6.2 CONTROL DE CAMBIOS

Los cambios en los procesos de producción, procedimientos y sistemas deben estar estrictamente limitados y bien controlados. Sólo cambios autorizados, probados y documentados (incluyendo en todos los casos la evaluación de riesgos) son permitidos en el ambiente de producción. Para la realización, pruebas, aprobación y aplicación en

producción de cambios, debe existir una adecuada segregación de funciones y separación de ambientes para promover y garantizar la integridad de estos.

Todos los cambios de alto impacto a los procesos de producción, procedimientos y sistemas deben ser aprobados por el Comité de Presidencia.

Se debe asegurar que los cambios de bajo impacto realizados sobre servidores y estaciones de trabajo, no comprometen los controles de seguridad corporativos y particulares establecidos en cada caso.

Todo cambio en la infraestructura tecnológica de Powerdata que impacte el cumplimiento normativo de la organización (p.ej. PCI DSS), debe socializarse en el Comité de Control de Cambios. Estos cambios deberán contar con la aplicación de los controles necesarios para evitar desviaciones en el cumplimiento normativo de la organización.

6.3 SEGREGACIÓN DE FUNCIONES

Es responsabilidad de los líderes de áreas asegurar que existe una adecuada segregación de funciones entre sus colaboradores, incluido el acceso a sistemas y redes. El acceso debe concederse solamente al personal apropiado y aprobado, basado en las necesidades del negocio. Todas las funciones deben asignarse de modo que se minimice la oportunidad de ocultar errores o irregularidades por parte de los colaboradores asignados. El acceso a los ambientes de producción debe estar limitado, monitoreado y aprobado según los procedimientos definidos para estos efectos.

6.4 SEPARACIÓN DE AMBIENTES

Powerdata debe implementar entornos de producción adecuadamente separados de los entornos de desarrollo y prueba. Como mínimo, estos ambientes deben ser lógicamente separados. Los datos de producción no deben ser utilizados en entornos de desarrollo o prueba a menos que su uso esté debidamente garantizado y que tal uso sea compatible con la legislación aplicable y las obligaciones contractuales.

6.5 PLANEACIÓN Y ACEPTACIÓN DE SISTEMAS

Los administradores de telecomunicaciones y sistemas de Powerdata son responsables de asegurar que éstos cuentan con la capacidad y los recursos disponibles. Los cambios en los nuevos sistemas existentes deben ser probados de acuerdo con los criterios de aceptación definidos.

6.6 ADMINISTRACIÓN Y SEGURIDAD DE LOS MEDIOS DE ALMACENAMIENTO

Todos los colaboradores de Powerdata que tengan acceso a documentos en medios de almacenamiento, datos de entrada y salida, y documentación de los sistemas de almacenamiento deben protegerlos contra daño, robo y acceso no autorizado.

6.6.1 USO DE DISPOSITIVOS EXTRAIBLES DE ALMACENAMIENTO

El uso de dispositivos de almacenamiento extraíbles ha sido aprobado exclusivamente para acceso y uso de la alta gerencia (Directores, Gerentes, Vicepresidentes y Presidente) y a través de equipos asignados por Powerdata.

Cuando por necesidad del negocio, se requiere habilitar su uso a colaboradores de otros cargos, se debe generar un concepto de Seguridad de la Información donde se identifiquen los riesgos asociados a la necesidad y los respectivos controles de seguridad que eviten posibles incidentes de fuga de información u algún otro riesgo que aplique.

La información confidencial (datos de bases de datos) debe ser almacenada con cifrado fuerte.

6.6.2 DISTRIBUCIÓN DE MEDIOS DE ALMACENAMIENTO

Cada vez que sea necesario realizar el desplazamiento de algún medio de almacenamiento es importante tener presente:

- Realizar el envío por medio del proveedor de mensajería contratado por Powerdata y que permite el rastreo del paquete durante su transporte hasta la entrega del mismo. Una vez se confirme la entrega de dispositivo, dejar como evidencia del envío el certificado de entrega.

- De ser necesario acatar las recomendaciones realizadas por el proveedor del dispositivo con el fin de asegurar el transporte de tal manera que no afecte la disponibilidad e integridad de los datos almacenados durante el mismo.

- La distribución de medios donde se almacene información confidencial y de uso interno, debe ser aprobada por la gerencia del área que es responsable de esta información.

Para tener claridad frente a las actividades y políticas específicas para el envío y recepción de medios en las instalaciones de Powerdata, remitirse al procedimiento de Control de Acceso Físico (GIS82).

6.7 PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

Se debe asegurar que los controles de detección, prevención y recuperación para proteger la información contra códigos maliciosos sean implementados en todas las áreas de la compañía, los colaboradores de Powerdata deben reconocer la importancia de la implementación de dichos controles y apoyar su implementación.

Las directrices establecidas en Powerdata para la protección frente a software malicioso se encuentran descritas en el procedimiento Administración De Antimalware (TEC02).

6.8 RESPALDO DE INFORMACIÓN – BACKUP

Powerdata debe mantener la integridad y la disponibilidad de la información mediante procedimientos rutinarios que soporten el resguardo y restauración de la información de la compañía, registrando eventos de falla y monitoreando permanentemente el proceso. Las disposiciones para el resguardo de la información deben garantizar el cumplimiento de los requerimientos del plan de continuidad del negocio y el aseguramiento de la confidencialidad de la información contenida en estas. Las copias de seguridad deben almacenarse en un lugar seguro, servicio que podrá ser contratado por Powerdata con un tercero debidamente seleccionado.

Los lineamientos para la gestión de respaldo de la Información gestionada en Powerdata se encuentran en el procedimiento Generación de Copias de Respaldo (TEC61)

6.8.1 BACKUP DE ESTACIONES DE TRABAJO

Todos los colaboradores de Powerdata que usen computadores de escritorio o portátiles son responsables de realizar las copias de seguridad de la información que consideren relevante contenida en los equipos con el fin de proteger los recursos de información de la pérdida o daños.

En adición, es responsabilidad del área técnica, definir y poner a disposición de los usuarios de computadores de escritorio y/o portátiles los mecanismos técnicos que permita garantizar el respaldo como mínimo de la información relevante contenida en los equipos.

Los lineamientos establecidos para Backus se encuentran descritos en el procedimiento Gestión de Backus PC (TEC119).

6.9 SEGURIDAD EN LAS REDES

Todas las redes de Powerdata deben ser diseñadas y administradas para garantizar la disponibilidad, fiabilidad y salvaguardar la red de Powerdata. Las redes deben incorporar zonas de seguridad para proporcionar niveles de seguridad para los datos y herramientas de red, generando una adecuada segmentación entre los diferentes ambientes y los servicios.

Para robustecer los niveles de seguridad de la red, es fundamental contar con la protección de un Firewall de red en los siguientes escenarios:

- Conexiones desde la red interna hacia internet y viceversa.
- Conexiones desde la red interna hacia redes desmilitarizadas (DMZ).

Las directrices establecidas en la compañía para este fin están descritas en las guías de configuración segura (hardening) para cada componente de red.

6.9.1 SEGURIDAD EN REDES INALÁMBRICAS

Para garantizar el acceso a los recursos de Powerdata desde dispositivos con conexión inalámbrica se ha dispuesto que existan redes inalámbricas administradas por la Gerencia de Infraestructura y Telecomunicaciones.

Para garantizar la seguridad de la información que viaja a través de estas redes inalámbricas se debe implementar un control de acceso basado en autenticación fuerte, cifrado del tráfico a través de una tecnología que implemente criptografía sólida y separación de redes para colaboradores de redes para terceros y proveedores. Para conceder el acceso a un tercero, la solicitud la debe hacer el funcionario encargado, deberá estar aprobada por el Director o Gerente del Área y deberá contar con un concepto positivo de Seguridad de la Información.

Cada una de las redes de acuerdo a su propósito deberá tener un sistema de control de contenido, reglas de enrutamiento o políticas de firewall que limite su conectividad únicamente a otros segmentos de red, redes o equipos a los que se requiera. Así mismo únicamente deberán irradiarse en las áreas físicas en donde se requieran, evitando hacerlo en sitios de alta confidencialidad como Centros de Datos.

Por considerarse una tecnología crítica dentro del cumplimiento de PCI DSS, la configuración de las redes inalámbricas deberá cumplir las políticas de este documento en el numeral 11.2.6.

6.10 INTERCAMBIO DE INFORMACIÓN Y SOFTWARE

El intercambio de información y software entre Powerdata y otras organizaciones debe ser controlado y ser consecuente con las políticas y legislación aplicable. Para tal fin, establece acuerdos basados en estándares y procedimientos para proteger la información y los medios de tránsito al momento de compartirla. Se deben considerar las implicaciones comerciales y de seguridad relacionadas con el intercambio electrónico y/o por medios físicos de datos, el comercio electrónico y el correo electrónico.

Antes que la información sea publicada electrónicamente el propietario de la información con el apoyo de las áreas de soporte técnico, debe garantizar que esta tiene la protección necesaria para prevenir la modificación no autorizada; esta información debe cumplir con las leyes, normas y estatutos de la jurisdicción en la cual se localiza el sistema, o en la cual se causa la transacción.

Se deben establecer acuerdos de custodia de software, notificación de envío y recepción, en los casos en los cuales sea necesario. Igualmente, se deben seguir las normas para armado de paquetes, rotulados de medios, responsabilidades y obligaciones en caso de pérdida de los datos expresadas en la política de gestión de activos.

6.11 TRANSMISIÓN ELECTRÓNICA DE DATOS

Para la transmisión electrónica de información, a través de redes públicas, inalámbricas, celulares y/o internas, entre POWERDATA y cualquier otra persona u organización se debe contar con la implementación de controles necesarios de acuerdo con la clasificación de la información (Pública, Interna y/o Confidencial) con el fin de minimizar los riesgos en los equipos de cómputo, redes y datos.

Para toda información cuya clasificación sea CONFIDENCIAL, deberán utilizarse tecnologías de cifrado (certificados o llaves) bajo algoritmos de cifrado fuertes, con versiones y configuración seguras, que sean aceptados por la industria, que no presenten vulneraciones y que estén de acuerdo con las políticas de clasificación de información y cifrado (algunos métodos de cifrado permitidos son: IPSec, AES256, 3DES a triple longitud, SHA256, etc.); en todos los casos de deben aplicar las normas establecidas por el estándar de seguridad de la industria de pagos (PCI DSS).

6.12 EQUIPOS MOVILES QUE CONTIENEN INFORMACIÓN DE POWERDATA

Todos los equipos móviles de propiedad de POWERDATA que contengan información de POWERDATA deben ser asegurados física y lógicamente cuando estén desatendidos. De igual forma, en estos equipos se deben instalar herramientas que permitan el cifrado seguro de los medios de almacenamiento. Es responsabilidad del personal que tenga asignado un dispositivo móvil protegerlo dentro de lo razonable y sin infringir las Políticas existentes.

No se permite el almacenamiento de información de Powerdata en equipos móviles distintos a los asignados por Powerdata. Las políticas para el uso adecuado de estos dispositivos se encuentran Anexo Medidas de seguridad para dispositivos móviles.

De igual forma, a los dispositivos móviles corporativos, se les debe aplicar configuraciones de seguridad que se encuentren establecidas en guías de aseguramiento para este tipo de dispositivos antes de ser entregados al colaborador autorizado.

6.13 REGISTROS – LOGS

Los logs de operación, error o falla y eventos de seguridad deben ser mantenidos y revisados para todos los sistemas y operaciones críticas. Cualquier actividad sospechosa o inusual debe ser comunicada de conformidad con los procedimientos establecidos.

6.14 EVALUACIÓN DE VULNERABILIDADES, ACTUALIZACIÓN Y PARCHADO DE SISTEMAS

Powerdata ha establecido un proceso para identificar y mitigar las vulnerabilidades de seguridad en los sistemas, aplicaciones y redes de Powerdata el cual debe ejecutarse y cumplir con los requisitos de las normas de industria (PCI- DSS, 27001, entre otros), los requerimientos legales y regulatorios vigentes, incluyendo las actividades de identificación, evaluación, e incorporación de actualizaciones y parches a los sistemas para asegurar que se conocen las debilidades de seguridad y que se tratan en el momento oportuno.

Las directrices establecidas en Powerdata se encuentran descritas en el Procedimiento Gestión de Parches y Vulnerabilidades de Seguridad (TEC126).

6.15 LINEA BASE PARA CONFIGURACIÓN DE SEGURIDAD

Se debe establecer e implementar estándares de configuración segura (guías de hardening avaladas por la industria) para los sistemas de información, las bases de datos, servidores web, las aplicaciones, los equipos de telecomunicaciones, equipos de seguridad perimetral, entre otros, con el fin de asegurar los mínimos niveles de seguridad y control sobre la información en Powerdata.

Los estándares de configuración segura deben ser implementados en un activo antes de realizar su inclusión dentro de la red de Powerdata.

Para la protección de los datos confidenciales (datos de Interfaz de usuario del software de analítica POWER BI, información de reserva bancaria, entro otros) como mínimo se deben tener en cuenta las siguientes consideraciones a nivel de gestión e implementación de normas de configuración segura de todos los sistemas:

- Definir los procedimientos de configuración y endurecimiento (hardening) para todos los componentes de sistemas, incluyendo sistemas operativos, aplicaciones, servidores web, servicios, productos y dispositivos de comunicaciones, etc.

- Todos los procedimientos de configuración definidos deberán contener Guías de Configuración Segura específicas que contemplen todas las vulnerabilidades conocidas y sean coherentes con las normas de aseguramiento aceptadas en la industria, como por ejemplo las especificadas por SysAdmin Audit, Network Security Network (SANS), el National Institute of Standards Technology (NIST), y el Center for Internet Security (CIS).

- Se deberá ajustar el endurecimiento (hardening) de los componentes de sistemas siempre y cuando se identifiquen vulnerabilidades técnicas conocidas que obliguen a la modificación de parámetros (a un nivel más robusto) para el cierre de brechas de seguridad.

- Las áreas de la organización encargadas de la implementación de las guías de configuración segura deberán documentar la aplicabilidad de cada uno de los parámetros mínimos indicados en dichas guías. En caso que el parámetro indicado “no aplique”, se deberán justificar detalladamente tanto las razones de negocio como técnicas que soporten su no aplicabilidad.

- Los parámetros de las guías de configuración segura que no puedan implementarse por razones tecnológicas deberán controlarse a partir de la definición, implementación y documentación de controles compensatorios que

permitan disminuir cualquier riesgo de seguridad sobre el sistema de información involucrado.

- Los procedimientos de configuración y Guías de Configuración Segura deberán incluir al menos lo siguiente:

    - Cambiar siempre los valores por defecto o de fábrica antes de su instalación en el entorno. Algunos ejemplos de valores por defecto pueden ser contraseñas, comunidades SNMP inseguras, cuentas innecesarias, etc.

    - Implementar solamente una función primaria por servidor (por ejemplo, los servidores de Web, servidores de base de datos y servidores de nombre de dominio (DNS) se deben implementar como servidores separados).

    - Deshabilitar todos los servicios y protocolos innecesarios (servicios y protocolos que no sean directamente necesarios para realizar la función especificada de los dispositivos).

    - Configurar los parámetros de seguridad del sistema para prevenir el uso indebido.

    - Eliminar todas las funcionalidades innecesarias, tales como archivos de comandos (scripts), funciones, subsistemas, sistemas de archivo y servidores de Web innecesarios.

    - Cifrar todo el acceso administrativo que no sea de consola con tecnologías como HTTPS, SSH, VPN, o TLS (en su última versión) para la administración Web y otros tipos de accesos administrativo sin consola.

    - Procesos para la adquisición y distribución de la hora correcta en todos los componentes de sistema.

    - Todos los procedimientos de configuración y Guías de Configuración Segura deberán actualizarse continuamente con base en nuevas versiones, parches de seguridad, parámetros de configuración o criterios establecidos durante el análisis y especificación de los requerimientos de seguridad. Para ello, será necesario establecer procedimientos que garanticen la identificación de nuevas vulnerabilidades para todos los componentes de sistema.

    - No se permite la utilizar para conexión ningún puerto inseguro como Telnet, FTP, Http, SNMP, entre otros.

6.16 SINCRONIZACION DE HORA

Los servidores NTP de Powerdata deben recibir señales de tiempo de fuentes externas que a su vez se basen en la hora atómica internacional o UTC. De igual forma, éstos servidores NTP (mínimo dos o tres) deben ubicarse en una red interna.

7 CONTROL DE ACCESO

Lineamientos para el control de acceso a la información.

7.1 SOLICITUD DE REQUERIMIENTOS DE ACCESO

Todos los accesos y privilegios a los datos del negocio y los sistemas de información de Powerdata deben estar debidamente autorizados y documentados antes que el acceso se pueda conceder.

Los lineamientos relacionados con la aprobación, modificación y terminación de accesos en los sistemas de información se encuentran descritos en el procedimiento Gestión de Usuarios (TEC134).

7.2 REQUERIMIENTOS DE NEGOCIO PARA ACCESO LÓGICO

El acceso lógico de las áreas del negocio a los datos y sistemas de información de Powerdata, debe contemplar como mínimo:

- Los requisitos del negocio,
- Las funciones de los colaboradores descritas en los descriptores de los cargos,
- Los privilegios de acceso definidos en las matrices de roles y perfiles de los sistemas de información,
- Los requerimientos de seguridad que se deben considerar en los sistemas de información y
- El concepto de “Menor privilegio”, es decir, proveer solamente aquellos accesos necesarios para desempeñar una función asignada.
- El registro y aprobación de la asignación de los accesos a los datos y sistemas de información de Powerdata de acuerdo con lo establecido en el Procedimiento de Gestión de Usuarios (TEC134).

Todo acceso web que permita conexión a los administradores debe estar cifrado. Los administradores no deben acceder mediante protocolos inseguros a sus sistemas (Servidores, bases de datos, equipos de red).

El acceso a los aplicativos de Powerdata y sus funcionalidades debe ser controlado adecuadamente incluyendo, pero no limitado a:

- La información que reside en los sistemas
- Utilitarios del Sistema
- Código fuente
- Ejecutables
- Librerías de desarrollo, pruebas y producción

Se deben implementar controles que permitan que un usuario sea eliminado después de presentar 90 días de inactividad. De no poder implementar un control que permita eliminar las cuentas de usuarios, el administrador funcional de la aplicación debe realizar una revisión trimestral, donde se garantice la revisión y eliminación de los usuarios con este periodo de inactividad. Es necesario dejar evidencia de la parametrización en la aplicación o la revisión y borrado realizado manualmente.

7.2.1 USO DE DISPOSITIVOS NO AUTORIZADOS PARA ACCESO A LA RED

No se permite la conexión a la red a través de dispositivos diferentes a los dispuestos por Powerdata. Cualquier dispositivo como tarjetas de red LAN, inalámbrico, routers y puntos de acceso inalámbrico deben estar restringidos para uso dentro de las instalaciones de Powerdata.

Incidentalmente se permite el uso personal de estos dispositivos en equipos diferentes a los de Powerdata, siempre y cuando no comprometa la seguridad de la red interna y de la información. Para las áreas donde se maneja información confidencial debe estar restringido el uso e ingreso de estos dispositivos.

7.3 CONTROL DE ACCESO REMOTO

El acceso remoto externo a la plataforma tecnológica de Powerdata por parte de colaboradores y terceros debe ser restringido. De ser requerido, siempre y cuando no se comprometa la seguridad de la información, se podrá otorgar bajo las siguientes condiciones:

- Todo acceso remoto deberá solicitar un mecanismo de doble autenticación. Cuando se utilice contraseñas, estas deberán cumplir con las características de complejidad de contraseñas que Powerdata haya definido.

- En principio, este acceso se podrá otorgar a usuarios internos cuyo rol sea el brindar soporte a las herramientas o sistemas de información de Powerdata. Si

el usuario que requiere acceder remotamente no pertenece al rol ya mencionado, a través de un concepto de seguridad de la información, se deberá analizar el requerimiento el cual deberá contar con una justificación de negocio.

- Los accesos remotos de terceros y/o proveedores de servicio deberán otorgarse mediante una sesión webex. Si un tercero y/o proveedor de servicio requiere de una conexión remota fija (p. ej. Administración tercerizada de infraestructura tecnológica), estos deberán contar con una justificación de negocio y doble factor de autenticación para acceder a los sistemas de Powerdata. Dicho acceso deberá realizarse por medio de un equipo de salto para evitar que la infraestructura tecnológica del tercero/proveedor haga parte del alcance PCI DSS de Powerdata.

- Es responsabilidad de los dueños de proceso y/o responsables de aplicación, notificar oportunamente la eliminación de accesos remotos de terceros y/o colaboradores Powerdata, una vez finalice los tiempos contractuales, cambio de rol o se determine que ya no es necesario para la operación.

- Cualquier acceso requerido debe contar con justificación y autorización por parte del director o coordinador delegado/Gerente/Vicepresidente, vigencia de acceso y registro.

- No se permite el acceso remoto a terceros en los ambientes de producción ni en ambientes transaccionales, a menos que el objeto de su contrato lo requiera.

- Todos los accesos deben dejar registro de las actividades realizadas durante la conexión remota.

- Todas las conexiones remotas de terceros y/o proveedores de servicio deben expirar después de uso.

- Todos los accesos remotos requeridos deben contar con filtros por cargo y/o nivel de acceso.

- Todos los accesos remotos deben hacerse a través de las herramientas seguras dispuestas por la compañía.

- El acceso remoto se permite solamente desde equipos con las siguientes herramientas instaladas:

    - Control de Fuga de Información (DLP).
    - Antimalware con actualizaciones automáticas.
    - Últimas actualizaciones de seguridad instaladas.

- Bloqueo de dispositivos USB y CD/DVD escritura.
- El registro de conexiones remotas (logs de la aplicación) debe estar integrado con la herramienta de monitoreo (aplica para estaciones de trabajo de Powerdata).

- Se deben generar alertas de monitoreo que permitan la identificación de cualquier comportamiento anormal.

- El acceso remoto podrá ser revocado sin previo aviso en caso de identificarse su uso indebido o actividades sospechosas.

- El acceso remoto deberá ser configurado para que ante inactividad durante un periodo no mayor a 15 minutos cierre la sesión y requiera reautenticación por parte del usuario.

Los lineamientos donde se describe todo el proceso y políticas para la solicitud, creación y aprobación para colaboradores y terceros, se encuentran documentadas en el procedimiento Acceso Seguro para Soporte Tecnológico a Servicios de Misión Crítica y Acceso Seguro WEBEX.

7.4 CONTROL DE ACCESO EQUIPOS MÓVILES

No se permite la conexión de equipos móviles a la red corporativa de Powerdata. Si por alguna razón es requerido, se debe contar con concepto de Seguridad de la Información de acuerdo con los lineamientos establecidos en el procedimiento de Gestión de Usuarios (TEC134).

8 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

8.1 PROCESOS DE NEGOCIO

Los colaboradores de Powerdata deben seguir los procesos para desarrollo y mantenimiento de sistemas debidamente aprobados.

8.2 AMBIENTES

Todas las aplicaciones que soportan las operaciones de Powerdata requieren como mínimo la existencia de ambientes independientes de desarrollo, pruebas y producción. En caso de existir impedimentos para dicha separación, se deben definir controles compensatorios aprobados por el Comité de Procesos y Riesgos y en cumplimiento con el estándar PCI DSS, ISO27001 y mejores prácticas de la industria, de tal forma que mitiguen posibles incidentes de seguridad de la información.

Los datos de producción que se utilicen en un entorno distinto deben ser adecuadamente asegurados y protegidos, y su acceso debe ser limitado basado en clasificación de información.

8.3 DESARROLLO Y ADQUISICIÓN DE SISTEMAS

Deberá asegurarse que existan suficientes controles de seguridad durante el proceso de desarrollo o durante la fase de análisis de todo proyecto para crear, mejorar o adquirir un sistema.

8.4 SEGURIDAD DE LOS SISTEMAS Y ARCHIVOS DE SISTEMAS

Cuando se desarrolle, adquiera o modifiquen sistemas, los propietarios de la información y de los sistemas deberán asegurar que se apliquen controles de seguridad adecuados de acuerdo a la clasificación de la información procesada y/o almacenada.

9 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

9.1 DETECCIÓN Y REPORTE DE INCIDENTES

Los colaboradores de Powerdata deben estar atentos a los riesgos y vulnerabilidades que puedan afectar la integridad, confidencialidad de la información y reportar las posibles ocurrencias tan pronto como sea posible. Powerdata debe seguir los lineamentos para registrar, responder y divulgar la información necesaria relacionada con incidentes de seguridad y ciberseguridad, de acuerdo con lo establecido en el Manual para la Gestión de Incidentes de Seguridad de la Información (CIS91-MA01). Se concederá el anonimato a los individuos que divulguen incidentes causados por otro colaborador.

9.2 GESTIÓN DE INCIDENTES

Los incidentes de Seguridad de la información y ciberseguridad son investigados por personal calificado, que proceda a la correcta identificación de las causas para así prevenir futuras ocurrencias, la coordinación de dichas actividades es efectuada por la Dirección de Seguridad de la Información según lo descrito en el Manual para la Gestión de Incidentes de Seguridad de la Información (CIS91-MA01). La evaluación de los mismos debe realizarse acorde a las circunstancias particulares; lo cual puede requerir o no la acción de varias áreas o departamentos. La evidencia debe ser recolectada adecuadamente.

9.3 REPORTE A TERCERAS PARTES

Los incidentes de seguridad de la información y ciberseguridad, que estén relacionados con requerimientos legales o regulaciones deben ser reportados a autoridades externas por personas autorizadas de Powerdata. Así mismo, cuando sea necesario y de acuerdo con los términos establecidos para el efecto en la Ley, Powerdata debe divulgar a las autoridades competentes, cuando tenga conocimientos de violaciones a la normatividad o reglamentación que él es aplicable. Por otra parte cuando se necesario se aplicarán sanciones disciplinarias acorde a la falta cometida.

Los incidentes de seguridad de la información y ciberseguridad, que estén relacionados con información de entidades miembros deben ser reportados a las entidades comprometidas por personas autorizadas de Powerdata.

Los incidentes de seguridad de la información y ciberseguridad, que estén relacionados con información de licencias de Power BI deberán ser reportada a las diferentes marcas y/o consumidores de pymes por las personas autorizadas de Powerdata.

Los incidentes de seguridad de la información y ciberseguridad que afecten de manera significativa la confidencialidad, integridad o disponibilidad de la información deben reportarse a la Superintendencia Financiera de Colombia haciendo una breve descripción del incidente, su impacto y las medidas adoptadas para gestionarlo. De igual forma, este tipo de incidentes deberán reportarse a las autoridades que hacen parte del modelo nacional de gestión de incidentes cibernéticos (Ejm: COLCERT, csirt PONAL, etc), con el fin de fortalecer las bases de conocimiento y buenas prácticas para la gestión oportuna de incidentes de seguridad de la información y ciberseguridad.

9.4 ANALISIS FORENSES DE SEGURIDAD DE INFORMACIÓN Y CIBERSEGURIDAD

Se debe tener un proceso de análisis forense de seguridad de información para apoyar la gestión de incidentes. El proceso debe ocuparse de la legislación aplicable para la recopilación de pruebas en apoyo de la admisibilidad, la calidad, y la exhaustividad de las pruebas.

10 CUMPLIMIENTO

Establece estrategias para evitar el incumplimiento de cualquier ley y/o disposición reglamentaria o contractual que incorpore obligaciones relacionadas con seguridad de la información y ciberseguridad.

10.1 CONFORMIDAD CON LAS LEYES Y REGULACIONES

Todas las políticas de seguridad de la información y ciberseguridad deben obedecer a las leyes aplicables, tal como leyes asociadas a la protección de los datos personales, protección de la información personal y documentos electrónicos, normas relativas a la de seguridad de datos de la industria de medios de pago, reglamentación de ciberseguridad y ciberdefensa, etc., las cuales se entienden incorporadas a esta política y prevalecen sobre éstas.

Las políticas de seguridad y el sistema de gestión de seguridad definidos, velan por el cumplimiento a los requerimientos y a la regulación establecida por la Superintendencia Financiera de Colombia, Superintendencia de Industria y Comercio, la ISO 27001 y la gestión de DBMS y demás aplicables.

10.2 ACCIONES DISCIPLINARIAS POR INCUMPLIMIENTO

En caso que por negligencia o intención, los colaboradores incumplan los procedimientos o normas de seguridad de información establecidas, serán reportados por el área de auditoría y/o la Dirección de Seguridad de la Información directamente a Presidencia, donde con la participación de la Gerencia de Talento Humano, se determinarán las sanciones a que haya lugar de acuerdo con la gravedad de la situación presentada, se podrá dar lugar a la terminación del vínculo laboral de acuerdo con la legislación y se establezca como justa causa o incluso a la toma de medidas judiciales y/o penales de acuerdo con el caso y en tanto se cuenten con los elementos probatorios.

10.3 DERECHOS DE PROPIEDAD INTELECTUAL

Powerdata cumple la normatividad legal relacionada con el uso de material protegido por los derechos de autor y de propiedad intelectual y el cumplimiento de los acuerdos de licenciamiento de software. En todos los casos el uso y/o almacenamiento de copias ilegales de software y/o de cualquier otro tipo de material protegido por derechos de autor en activos de información de Powerdata está prohibido.

10.4 COMPROMISOS A LA SEGURIDAD

Toda actividad destinada a uso indebido o a obtener acceso no autorizado a sistemas sensibles y/o información clasificada como confidencial se encuentra expresamente prohibida en Powerdata, incluyendo, pero no limitándose a:

- La posesión, el uso, o la descarga de herramientas que tratan de violar la protección de los derechos de autor de software, la captura de tráfico de red,

descubrir contraseñas, identificar vulnerabilidades de seguridad, o descifrar archivos cifrados.

- El uso de la ingeniería social para comprometer la seguridad

Los colaboradores que utilicen este tipo de herramientas de diagnóstico deben recibir la aprobación previa por escrito de los responsables de la seguridad de la información. En todos los casos las actividades de mantenimiento que requieren el uso de herramientas de diagnóstico deben seguir los procedimientos de gestión de cambio.

10.5 PROTECCIÓN A INFORMACIÓN PERSONAL Y PRIVADA

Powerdata cumple con la legislación aplicable en temas de protección a la privacidad y garantiza que los riesgos se reducen al mínimo en aquellos casos en que se requieran datos que están sujetos a protección.

10.6 DERECHO A MONITOREAR

Con el fin de asegurar el cumplimiento de las políticas, Powerdata se reserva el derecho a monitorear las actividades ejecutadas por sus colaboradores, como parte de sus responsabilidades dentro de la operación, cuando sea requerido por necesidad del negocio o por requerimientos legales dando cumplimiento a la máxima extensión permitida por las leyes aplicables.

Adicional, el personal de Powerdata no debería tener expectativa de privacidad asociada con información que se almacena o se envía a través de los sistemas de información de Powerdata, o se almacena en las instalaciones de Powerdata.

Los sistemas de información están sujetos a dicho examen incluyen, pero no se limita al correo electrónico, archivos del sistema, archivos en las unidades de disco de los computadores, archivos de mensajes de voz, archivos de spool de impresora, fax y máquinas de producción.

Powerdata se reserva el derecho deliminar de sus sistemas de información cualquier material que considera ofensivo o potencialmente ilegal, además se reserva el derecho de pedir a los colaboradores al momento de salir de las instalaciones revelar el contenido de cualquier bolso o paquete.

Powerdata podrá optar por utilizar herramientas software u otros dispositivos para ayudar a las mencionadas actividades de vigilancia. Se prohíbe a los colaboradores desactivar estas herramientas o interferir en su funcionamiento.

10.7 REVISIÓN AL CUMPLIMIENTO

Powerdata realiza revisiones de cumplimiento a las políticas y normas de seguridad para garantizar su aplicación consistente. El área de Auditoría Interna o una firma externa calificada lleva a cabo estas revisiones basadas en el riesgo relativo y de conformidad con las mejores prácticas de auditoría.

10.8 CUMPLIMIENTO DE TERCERAS PARTES

Todos los terceros que tengan acceso a activos protegidos de los cuales Powerdata es propietario, posee o administra deben cumplir con las políticas, normas y procedimientos de seguridad.

11 CUMPLIMIENTO DE LA GESTIÓN DE BASES DE DATOS (DBMS)

11.1 OBJETIVO Y ALCANCE

Esta sección tiene como objetivo establecer las pautas a seguir en Powerdata para garantizar la debida protección de los datos del software de analítica de datos de sus clientes, así como el cumplimiento de cada uno de los requerimientos del estándar de bases de datos.

Estas políticas deben ser de común conocimiento por parte de todos aquellos colaboradores y/o terceras partes que la necesiten para el desarrollo normal de sus tareas en las que se trate con datos de Interfaz de usuario del software de analítica POWER BI.

Para facilitar el cumplimiento del Estándar PCI DSS, Powerdata ha definido un “Manual de Gestión de Cumplimiento – PCI DSS” el cual contiene: Directrices frente al cumplimiento del Estándar en mención, el desarrollo de cada una de las fases establecidas en la gestión del cumplimiento (Modelo de Gobierno PCI DSS), los roles y responsabilidades de cada uno de los actores involucrados en la gestión del cumplimiento PCI DSS de la organización.

11.2 DEFINICIONES

- ASV (Approved Scanning Vendor): Acrónimo de “Approved Scanning Vendor” (proveedor aprobado de escaneo). Empresa aprobada por la industria PCI SSC para prestar servicios de análisis de vulnerabilidad externa.

- Cifrado: Proceso que consiste en transformar la apariencia de los datos para volverlos ininteligibles para todos aquellos que no posean una clave criptográfica

específica. El cifrado evita que la información cifrada y descifrada (proceso contrario al cifrado) sea revelada a personas no autorizadas.

- Cifrado de Base de Datos por Columna: Técnica o tecnología (software o hardware) utilizada para cifrar el contenido de una columna específica en una base de datos, en lugar de toda la base de datos. Como alternativa, consulte Cifrado de disco o Cifrado por archivo.

- Cifrado de Disco: Técnica o tecnología de software o hardware que se utiliza para cifrar todos los datos almacenados en un dispositivo (por ejemplo, un disco duro o una unidad flash). Además, los contenidos de archivos o columnas específicas pueden cifrarse mediante el cifrado por archivo o el cifrado de base de datos por columna.

- Cifrado por Archivo: Técnica o tecnología de software o hardware que se utiliza para cifrar todo el contenido de archivos específicos. Como alternativa, consulte Cifrado de disco o Cifrado de base de datos por columna.

- Clave: En criptografía, la clave es un valor que determina el resultado de un algoritmo de cifrado al transformar texto simple en texto cifrado.

- Componentes del Sistema: Todo componente de red, servidor o aplicación que se incluye en el entorno de datos del titular de la licencia de POWER BI o está conectado a él.

- Desmagnetización: Método para purgar la mayoría de los soportes magnéticos. Se trata de un proceso mediante el cual el soporte de datos magnéticos es eliminado, retornando a su estado inicial.

- Formateo de Bajo Nivel: Proceso de preparación del disco o soporte de datos sobrescribiéndolo con información en blanco.

- Hash: Es una función o método para generar claves que representen de manera casi unívoca a un documento, registro, archivo, etc., utilizando una función hash o algoritmo hash. Un hash es el resultado de aplicar dicha función o algoritmo.

- Incidente de Seguridad de la información: Cualquier anomalía que pueda producirse esporádicamente y que afecte o pueda afectar a la seguridad de los datos, entendida esta seguridad en sus aspectos de confidencialidad, integridad, disponibilidad, identificación y autenticación.

- Pueden ser tanto físicas (fuego, inundación, acceso no autorizado a zonas restringidas, etc.) como lógicas (infección por virus, revelación de passwords, etc.).

- MD5: Es un algoritmo de reducción criptográfico de 128 bits de tamaño. Este algoritmo es considerado como inseguro, teniendo en cuenta que ya fue comprometido su método criptográfico.

- Pista de Auditoría: registro de actividades realizadas por los usuarios sobre los sistemas de información y bases de datos que permite al auditor tener conocimiento de qué ha sido realizado por cada usuario y cuándo se ha ejecutado dicha acción.

- QSA (Qualified Security Assessor): Acrónimo de “Qualified Security Assessor” (evaluador de seguridad certificado), empresa autorizada por el PCI SSC para realizar evaluaciones in situ del cumplimiento de las normas PCI DSS.

- Soporte de Datos: Se entiende por soporte de datos todo equipo o medio donde se almacena la información con independencia de que el dispositivo físico y la tecnología empleada sea magnético, óptico o cualquier otro.

- Se ha de tener presente que los ordenadores personales, incluyendo ordenadores portátiles, agendas electrónicas, etc., con discos duros y otros dispositivos de almacenamiento no volátil, operando de forma aislada o conectados a la red, se han de considerar como medios de almacenamiento de información en el mismo sentido que otros soporte de datos extraíbles.

- Wipe: Mecanismo de borrado de información que sobrescribe la información de forma reiterada para prevenir su recuperación por medios no convencionales.

11.2.1 SEGURIDAD ASOCIADA AL RECURSO HUMANO

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal, desde su contratación y de manera continua, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento. Por esto el objetivo de esta política contiene:

- Reducir los riesgos de error humano, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

- Especificar las responsabilidades en materia de cumplimiento PCI DSS en la etapa de selección de personal e incluirlas en los acuerdos a firmar y verificar su cumplimiento durante el desempeño del colaborador.

- Garantizar que los colaboradores estén al corriente de las amenazas y actividades en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la Información en el transcurso de sus tareas diarias.

- Establecer Compromisos de Confidencialidad con todo el personal en el alcance de la certificación PCI DSS.

- Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

11.2.2 SEGURIDAD PARA EL MANEJO DE PROVEEDORES

Se establecen las normas para administrar correctamente la seguridad relacionada con el personal externo que presta servicios a Powerdata de forma temporal o permanente, ya sea en las instalaciones de Powerdata o desde las instalaciones de la empresa contratada.

11.2.3 GESTIÓN DE PROVEEDORES

De acuerdo a lo descrito en el procedimiento Selección, Evaluación y Reevaluación de proveedores (GCM190), para todos los terceros con los que se compartan datos de los el software de analítica de datos (por ejemplo, instalaciones de almacenamiento de cintas de respaldo, proveedores de servicios administrados como empresas de alojamiento Web o proveedores de servicios de seguridad, o aquellos que reciben datos a efectos de modelar la detección de fraudes) se debe realizar lo siguiente:

- Se debe tener documentada la lista de terceros con los cuales se comparten datos de los el software de analítica de datos.

- Debe existir un acuerdo escrito que incluya el reconocimiento por parte del tercero sobre su responsabilidad para mantener la seguridad de los datos del dashboard u otros datos confidenciales a los que tenga acceso.
- Antes de contratar a un tercero, se debe realizar la debida diligencia para asegurarse que la entidad sigue todos los requisitos de PCI aplicables para los servicios que provee.
- Al menos una vez al año, la lista de terceros deberá ser revisada. Un seguimiento de todos los terceros que manejan datos del software de analítica de datos deberá ser realizado para verificar que la conformidad con PCI DSS aún está vigente.

Los lineamientos para realizar la clasificación de proveedores de acuerdo a la norma PCI DSS, se encuentra en el anexo Manual de Seguridad de la Información para Manejo de Proveedores (GCM190-AN04).

11.2.3.1 CONTROL DE ACCESO PARA PROVEEDORES NIVEL 2 CON ACCESO LÓGICO A ACTIVOS QUE MANEJAN DATOS CONFIDENCIALES SIN ACCESO A LOS DATOS CONFIDENCIALES A LOS DATOS CONFIDENCIALES

Los accesos realizados por proveedores de nivel 2 pueden suponer un riesgo de seguridad en caso de no ser debidamente asegurados. Por este motivo, los administradores deben asegurar el cumplimiento de las siguientes medidas de seguridad:

- No enviar información sensible en los casos abiertos con proveedores: Esta información sensible incluye tanto datos del software de analítica de datos como contraseñas o cualquier información no necesaria para el caso y que aporte información sobre el entorno.

- En el caso de ser necesario el establecimiento de una sesión webex, los administradores mantendrán el control sobre sus máquinas no permitiendo que este pase al proveedor (el cuál actuará siempre en modo lectura) y estando presente en todo momento durante la sesión.

- Cuando el acceso del proveedor se realiza de forma presencial en las instalaciones de Powerdata, dicho acceso y cualquier acción ejecutada por el mismo deben ser realizados ante la presencia del administrador del sistema, a través de un usuario temporal habilitado únicamente el tiempo necesario para la operativa, siendo eliminado inmediatamente después de que haya finalizado la misma.

11.2.4 TRATAMIENTO DE LOS DATOS DEL SOFTWARE DE ANALÍTICA DE DATOS

Los datos relativos a Interfaz de usuario del software de analítica POWER BI se tratarán teniendo en cuenta las siguientes consideraciones:

- El responsable de definir los periodos de retención de los datos del software de analítica de datoss son los propietarios de la información (directores, Gerentes, vicepresidentes) de acuerdo con la normatividad legal vigente aplicable al sector financiero colombiano y de industria y comercio. Como base inicial y según la normatividad colombiana relacionada con la preservación de información financiera para fines de atención de reclamaciones y/o requerimientos en el sector, se determinará un periodo de retención de datos del software de analítica de datos de máximo 10 años, el cual podrá variar toda vez la normatividad y/o la legislación lo promuevan.

- Como mínimo cada 3 meses, los propietarios y/o custodios de los datos del software de analítica de datos deben revisar y depurar (de forma manual o automática) todos los archivos físicos y/o lógicos que contengan información de dashboard de Power BI y que hayan cumplido con los periodos de retención definidos en la organización. Si por algún motivo legal o de negocio se requiera almacenar los datos del software de analítica de datos por un periodo mayor al definido inicialmente, se deberá actualizar la tabla de retención de datos del software de analítica de datos y adicionalmente, revisar y/o fortalecer los controles de seguridad de dichos datos para asegurar su confidencialidad, integridad y/o disponibilidad.

- Debe existir un registro donde se identifiquen todos los sitios donde se está trabajando con información del software de analítica de datos en los diferentes medios (papel, cintas, bases de datos, digitalizados, archivos) como se describe en el instructivo Clasificación, Etiquetado y Protección de Información (CIS104-IN04) y a partir de allí, se debe establecer si se requiere o no toda la información. Adicional, se deben implementar controles para eliminar la información de forma automática, manual y periódica, de acuerdo a los periodos de retención definidos. Igualmente, es necesario realizar, por parte del responsable la información, una revisión trimestral de la efectividad de los controles definidos, para garantizar el borrado de los datos.

  Las áreas de negocio que requieran visualizar el dashboard de POWER BI deben justificar sus funciones, la necesidad de negocio y los controles que utilizarán para la protección de dicha información. Para esto, es necesario contar con un acta o algún otro tipo de registro que indique como mínimo lo siguiente:

i) ***los procesos***/subprocesos que hagan uso de dichos datos,
ii) ***los*** sistemas de información que lo requieren y

los controles definidos por la organización que mitiguen los riesgos de seguridad sobre dichos datos, se tomará como fuente los privilegios que se definan en las matrices de roles y perfiles de cada uno de los sistemas de información de Powerdata.

- No deben almacenarse datos confidenciales de autenticación después de la autorización (aunque estén cifrados):

- Los datos confidenciales de autenticación deberán borrarse de forma segura (mediante software de borrado seguro y/o comandos de borrado seguro en las plataformas donde se procesen dichos datos) una vez se realice el proceso de autorización.

- El número de cuenta primario o PAN, debe ser protegido de manera que se garantice su confidencialidad e integridad. El PAN debe ser ilegible en cualquier lugar donde esté almacenado (incluyendo datos en medios digitales portátiles, medios de respaldo, registros o logs) aplicando cualquiera de los siguientes métodos:

    - **One way hash basados en criptografía sólida**: Estos valores son apropiados cuando no es necesario recuperar el número original (son irreversibles).

    - **Criptografía sólida con Procesos y Procedimientos de Gestión de Claves Relacionadas:** El propósito de una criptografía sólida es que el cifrado esté basado en un algoritmo probado y aceptado en la industria (no en un algoritmo propietario o propio). Algunos ejemplos son: AES (256 bits y superior), RSA (2048 bits y superior), etc.

    - **Si se utiliza cifrado de disco** (en lugar de un cifrado de base datos por archivo o columna), se debe administrar un proceso lógico independientemente de los mecanismos de control de acceso del sistema operativo nativo (por ejemplo, no se deben utilizar bases de datos de cuentas de usuarios locales). Para cumplir con este requisito, el método de cifrado de disco no puede tener:

        - Una asociación directa con el sistema operativo.
        - Claves de descifrado asociadas con las cuentas de usuario.

- No se permite el almacenamiento de datos del software de analítica de datos en estaciones de trabajo, equipos portátiles, dispositivos móviles y medios extraíbles (USB, Discos externos, CD/DVD/, etc.). En Powerdata se ha dispuesto del File Server Seguro para almacenar esta información cuando sea requerido por necesidad del negocio.

11.2.5 BORRADO SEGURO

Toda la información confidencial (datos del software de analítica de datos, información de reserva bancaria, entre otros) debe ser eliminada de forma segura cuando ya no sea requerida o se haya cumplido su tiempo de retención.

El borrado seguro es un proceso que garantiza no permitir una recuperación de la información que se ha eliminado en cualquier medio de almacenamiento (discos duros de servidores y/o estaciones de trabajo, medios extraíbles, citas de backups, entre otros.

Para este proceso de borrado seguro, se deben utilizar las herramientas dispuesta por Powerdata para tal fin y generar un registro de lo realizado como se describe en el Instructivo de Saneamiento de Medios de Almacenamiento (CIS211-IN003).

11.2.6 USO DE TECNOLOGÍAS CRÍTICAS

Se consideran tecnologías críticas las redes inalámbricas, las tecnologías de conexión remota, servicios de correo electrónico, Internet y ordenadores portátiles.

El uso de dichas tecnologías críticas solo está permitido de la siguiente manera:

- Redes inalámbricas corporativas: Solo podrá utilizarse al interior de las instalaciones físicas de Powerdata y a través de los access point corporativos. Esto se limitará para los colaboradores que, por motivos de negocio, requieran desplazarse entre las diferentes áreas de la organización para ejecutar sus actividades diarias.
- Tecnologías de conexión remota: Su uso estará limitado para todo colaborador y/o tercero que por necesidad técnica y/o de negocio requiera conectarse remotamente tanto fuera como al interior de la red de Powerdata. Los accesos remotos estarán sujetos al uso de un múltiple factor de autenticación a los demás lineamientos descritos en el numeral 7.3 de las Políticas de Seguridad de la Información.
- Servicios de correo electrónico: Su acceso estará limitado a todo colaborador y/o tercero que por necesidades de negocio requieran conectarse al servidor de correo electrónico corporativo de Powerdata. Es de aclarar que no todas las

áreas del negocio podrán contar con acceso a este servicio debido a los requerimientos de los entes reguladores del sector financiero colombiano y de industria y comercio (ejm: Superintendencia Financiera de Colombia y Superintendencia de Industria y Comercio). De igual forma, se deberán cumplir los lineamientos establecidos en el numeral 3.8 de las Políticas de Seguridad de la Información.

- Servicios de impresión: Los colaboradores y/o terceros solo podrán hacer uso de los servicios de impresión distribuidos en las diferentes áreas de la organización. Los accesos a los servicios de impresión deberán otorgarse a través de la red interna de Powerdata. Según la criticidad y riesgo en la información de los procesos, el acceso a este servicio podrá restringirse a menos que se establezcan los controles necesarios según el concepto de la Dirección de Seguridad de la Información.
- Internet: El uso del servicio de navegación por internet solo se podrá otorgar para todo colaborador y/o tercero de Powerdata a través de la red interna de la organización. Los colaboradores de Powerdata solo podrán acceder a este servicio a través de su conexión con el directorio activo de la organización y los terceros de Powerdata lo podrán realizar de forma limitada a través de la red de proveedores (VLAN de proveedores). De igual forma, se deberán cumplir los lineamientos establecidos en el numeral 3.9 de las Políticas de Seguridad de la Información.
- Ordenadores portátiles: Su uso será únicamente de propósito corporativo y solo podrán conectarse a la red interna de Powerdata. El alistamiento de los ordenadores portátiles deberá contemplar configuraciones de seguridad necesarias para restringir su conexión a redes no confiables (Ejm: redes domésticas, redes públicas, redes de terceros, etc). De igual forma, se deberán cumplir los lineamientos establecidos en el numeral 3.6 de las Políticas de Seguridad de la Información.

El entorno afectado dentro del ámbito de PCI DSS deberá cumplir con las siguientes consideraciones:

- La utilización de dispositivos electrónicos extraíbles se encuentra restringida en Powerdata.
- El uso de estas tecnologías deberá requerir un esquema de autenticación como por ejemplo usuario/contraseña y/o multi-factor de autenticación.
- Se requiere aprobación explícita para el uso de estas tecnologías críticas por la respectiva Vicepresidencia.
- Se debe crear y mantener un listado de todos los dispositivos, productos aprobados por Powerdata y el personal que tiene acceso a ellos. Para cada uno de los dispositivos deberá especificarse los usos aceptados y la ubicación desde donde se autoriza su uso.
- Todos los dispositivos se etiquetarán indicando su dueño, información de contacto y propósito.

- Cualquier ordenador portátil que se conecte directamente a Internet y que se utilice para acceder a la red del entorno PCI DSS debe tener instalado un software de cortafuegos personal y antivirus gestionados.
- En los casos que se realicen conexiones remotas:
  - Deberán desconectarse automáticamente las sesiones después de un período específico de inactividad.
  - Cuando el acceso se realice por parte de proveedores, se activarán las tecnologías de acceso remoto solo cuando sea necesario y desactivarán inmediatamente después del uso.
  - Al acceder a datos a través de este tipo de conexión, no se almacenará información en los discos duros locales o cualquier otro medio externo. También se prohíbe el uso de funciones que permiten cortar y pegar e imprimir datos durante el acceso remoto.
  - Deberán definirse los procedimientos necesarios para garantizar el cumplimiento de los requerimientos expuestos.

Todos los accesos aprobados a tecnologías críticas deberán ser registrados de acuerdo con las definiciones de la Gerencia de Infraestructura y Telecomunicaciones.

11.2.7 LINEA DE COMANDOS

No se permite el acceso a la línea de comandos del sistema operativo, este acceso es exclusivo para acciones administrativas.

11.2.8 INSTALACIÓN Y MANTENIMIENTO DE CORTAFUEGOS Y ROUTERS

La configuración de los cortafuegos bloqueará todo el tráfico de redes y hosts “no confiables”, exceptuados los protocolos necesarios para el entorno de datos del software de analítica de datoss. Deberá realizarse una revisión semestral del conjunto de reglas de los cortafuegos y routers.

11.2.9 TRANSMISIÓN POR REDES PÚBLICAS

Toda conexión a una red pública que se establezca para la transmisión de datos del software de analítica de datos, debe implementar protocolos de seguridad y cifrado fuerte aprobados por la industria y bajo versiones y configuraciones seguras, como TLS v1.2 usando cifrado AES 256, HTTPS con certificados emitidos por una CA aprobada, FTPS con cifrado AES 256 o SFTP.

11.2.10 CONTROLES DE SEGURIDAD

Todos los sistemas, dispositivos de red y aplicaciones serán testeados frecuentemente para asegurar que los controles de seguridad se mantienen, pese a los cambios en el entorno. La correcta ejecución de los controles de seguridad se supervisará según lo establecido en el documento Pruebas Periódicas de Seguridad de la Información. Para ello, deberán implementarse las siguientes tareas y mecanismos:

- Realizar una auditoría de cumplimiento PCI DSS anualmente. Esta auditoría debe ser realizada por un proveedor QSA (Qualified Security Assessor). Los proveedores reconocidos como QSA por el PCI SSC se encuentran en el siguiente enlace: https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf.

- Realizar al menos trimestralmente, un monitoreo de puntos de acceso inalámbrico para identificar puntos de acceso inalámbricos presentes o un IDS/IPS inalámbrico capaz de identificar todos los dispositivos inalámbricos, generar alertas y detectar aquellos dispositivos inalámbricos no autorizados como se describe en el Procedimiento Monitoreo de Seguridad de la Información.

  Este análisis debe realizarse con la periodicidad especificada aunque no existan redes inalámbricas en el entorno que puedan contener datos de Interfaz de usuario del software de analítica POWER BI, ya que el objetivo es detectar dispositivos no autorizados.

- Se debe mantener un listado de redes/dispositivos wireless autorizados y conocidos en todos los Entornos PCI DSS, debido a la posibilidad que los clientes dispongan de este tipo de tecnología en su entorno y ampliar estos análisis a las salas en las que se ubica dicho servicio

- Realizar tests de intrusión internos y externos, de la infraestructura de la red y aplicaciones, al menos una vez al año, y después de actualizar o mejorar significativamente la infraestructura o cualquier aplicación.

  Dichos tests de intrusión deben incluir Pentest a nivel de red y de aplicación. Estos tests de intrusión pueden ser realizados por la Organización siempre y cuando el departamento que los realice sea completamente independiente del departamento a escanear o por un proveedor externo.

- Efectuar un análisis de riesgos formal, al menos anualmente, que permita identificar amenazas, vulnerabilidades y los riesgos asociados.

- Utilizar los sistemas de detección y/o prevención de intrusiones para supervisar el tráfico en el entorno de datos de titulares de la licencia de power BI y alertar al personal ante la sospecha de riesgos, y mantener actualizados todos los motores de detección y prevención de intrusiones, como se describe el procedimiento Administración del Sistema de Seguridad Perimetral (TEC16).

- Utilizar un software de monitorización de integridad de archivos para alertar al personal sobre cualquier modificación no autorizada de un sistema o contenido de un archivo de sistema crítico, ficheros de configuración o ficheros de contenido. El software debe estar configurado para realizar comparaciones de archivos críticos al menos semanalmente, como se describe en el procedimiento de Monitoreo de Seguridad de la Información (CIS176).

11.2.11 SISTEMA DE ADMINISTRACIÓN DE CONTRASEÑAS

Se deben utilizar sistemas interactivos para la administración de contraseñas que provean resultados de calidad. Las políticas de contraseñas seguirán las mismas directrices que para los casos anteriores teniendo también en cuenta:

- Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.
- Controlar la adición, eliminación y modificación de las identificaciones de usuarios, credenciales y otros objetos de identificación.
- Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.
- Modificar todas las contraseñas predeterminadas por el fabricante, una vez instalado el software y el hardware (por ejemplo sistemas operativos, claves de impresoras, switches, routers, etc.).
- Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.
- No se permite usar cuentas con contraseñas de grupo o compartidas explícitamente, solo es posible tener estos usuarios para proceso específicos, donde se documente su justificación, se asigne a un responsable especifico y se defina el almacenamiento de contraseña bajo control dual y conocimiento divido.
- En la implementación de los procedimientos de registro de usuarios y contraseñas establecidos deberán tenerse especialmente en cuenta las siguientes pautas:

    - Establecer la primera contraseña a un valor único por usuario y cambiarse inmediatamente después de su primer uso.
    - Establecer una debida verificación de la identidad del usuario antes de proceder a restablecer una contraseña.
    - Revocar inmediatamente el acceso a aquellos colaboradores que hayan cesado en sus funciones.
    - Eliminar o desactivar las cuentas de usuario inactivas al menos cada 90 días.

- Cambiar la contraseña al menos cada 30 días.
- Requerir una longitud mínima de 8 caracteres.
- Usar contraseñas que requieran caracteres numéricos y alfabéticos.
- Mantener un histórico de 12 contraseñas recordadas.
- Bloquear las cuentas de usuario tras un máximo de 3 intentos inválidos de acceso.
- Tras un bloqueo de cuenta, será el administrador el que deba desbloquear la cuenta.
- Requerir el bloqueo de la sesión tras un máximo de 15 minutos de inactividad, requiriendo una contraseña para la activación del terminal.

- Todos los accesos a bases de datos que contengan datos de titulares de Interfaz de usuario del software de analítica POWER BI, deberán ser autenticados debidamente incluyendo accesos por aplicaciones, administradores o cualquier otro usuario.

- Todas las contraseñas deberán ser cifradas durante su transmisión.

- Si se utilizan métodos de saneamiento físicos como tokens, el software de analítica de datoss inteligentes y/o certificados, estos deben ser asignados a una sola cuenta y deben garantizar que solo la cuenta asignada haga uso de estos para obtener el acceso entregado. En Powerdata este tipo de autenticación sólo es usado para el acceso remoto; el detalle de actividades y políticas para su asignación puede ser consultado en el procedimiento Acceso Seguro para Soporte Tecnológico a Servicios de Misión Crítica" (TEC251)

11.2.12 GESTION DE LLAVES DE CIFRAMIENTO

Las llaves y/o componentes de ciframiento deben ser administradas y custodiadas de forma segura, conservando los principios de control dual y cambio periódico de las mismas. El periodo de ciframiento de las llaves estará comprendido máximo hasta 3 años teniendo en cuenta posibles limitantes identificadas a través de una evaluación de riesgos lo cual podría afectar el tiempo de vigencia de los criptoperiodos. A continuación, se relacionan los factores que se deben contemplar en la evaluación de riesgos:

- La fortaleza de los mecanismos de cifrado (algoritmo utilizado, longitud de la llave, tamaño del bloque y modo de operación).
- El lugar donde se almacena la llave criptográfica.
- El volumen de transacciones.
- Tiempo de retención de los datos cifrados bajo llaves criptográficas.

- La función de la llave en los sistemas de información.
- Procesos o entidades que comparten la misma llave.
- Amenazas identificadas sobre la información que se está cifrando.

Las llaves de ciframiento fuera de servicio deberán ser desechadas de acuerdo con el proceso descrito en la Política de Retención y Eliminación de Datos. Si las llaves antiguas se deben mantener (para soportar datos archivados, encriptados, por ejemplo) deben ser fuertemente protegidas y usadas únicamente para propósitos de des ciframiento/verificación.

Adicional, los equipos criptográficos deben cumplir con los niveles de seguridad según estándar de industria y mejores prácticas de seguridad de la información.

11.2.13 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Deben identificarse, acordarse e incluirse los requerimientos de controles de seguridad de todos los sistemas en las especificaciones técnicas de todo nuevo sistema de información, modificación y/o ampliación de los existentes.

Cada líder de proceso o producto debe incorporar las especificaciones relacionadas con los requerimientos de controles automáticos y manuales que deben poseer los sistemas de información de Powerdata y elaborar los procedimientos de prueba y aceptación formal de los productos.

Consideraciones similares deben ser aplicadas cuando se evalúen paquetes de software, desarrollados internamente o a través de terceros.

Estos requisitos de seguridad y procesos para la implementación de la seguridad deben ser integrados en etapas tempranas de los proyectos de sistemas de información, dado que su introducción tardía es mucho más difícil y onerosa.

Los requisitos de seguridad y los controles deben reflejar el valor de los activos de información y el daño potencial o impacto derivado de la ausencia o falla en la seguridad.

11.2.14 ACTUALIZACIONES DE SEGURIDAD Y DESARROLLO SEGURO

Se deben establecerlas medidas de prevención para evitar al máximo la exposición de los sistemas a situaciones peligrosas. Para ello deben desarrollar aplicaciones de

software de acuerdo con PCI DSS, con base a las mejores prácticas de la industria que cumplan lo siguiente:

- Realizar pruebas de todos los parches de seguridad y cambios de configuración de software y sistema antes de implementarlos, incluyendo:
    - Validación de todas las entradas (para prevenir el cross–site scripting, los fallos de inyección, la ejecución de software malicioso, etc).
    - Validación del manejo apropiado de errores.
    - Validación del almacenamiento criptográfico seguro.
    - Validación de comunicaciones seguras.
    - Validación del adecuado control de acceso, basado en roles (RBAC).
- Todas las aplicaciones Web se deben basar en directrices de codificación segura establecidas por el Open Web Application Security Project – OWASP. Prevenir vulnerabilidades comunes de codificación en los procesos de desarrollo de software, incluyendo los siguientes:
    - Cross–Site Scripting (XSS): Validar todos los parámetros antes de ser incluidos.
    - Injection Flaws Particularmente SQL Injection: También pueden considerarse LDAP y Xpath. Validar la entrada de datos para que se puedan modificar el sentido de los comandos y de las consultas.
    - Ejecución de Ficheros Maliciosos: Validar la entrada para verificar que la aplicación no acepta nombres de archivos o ficheros procedentes de usuarios.
    - Referencias a Objetos Directos Inseguros: No exponer referencias a objetos internos a los usuarios.
    - Cross–Site Request Forgery (CSRF): No responder a los credenciales autorizados y fichas de forma automática, presentados en los navegadores.
    - Información de fallas y manipulación inapropiada de errores.
    - Autenticación y Gestión de Sesiones Rotas: Por ejemplo: manipulación de cookies de sesión.
    - Almacenamiento inseguro de la criptografía.

  - Comunicaciones Inseguras: Encriptar todas las comunicaciones autenticadas y sensibles, de forma adecuada.

  - Fallo en la Restricción de Accesos a URLs: Obligar a controlar el acceso en la capa de presentación y lógica del negocio para todas las URLs.

- Separar las responsabilidades o funciones entre los entornos de desarrollo, prueba y producción.

- Eliminar todos los datos y cuentas de prueba antes de activar los sistemas en producción.

- Eliminar cuentas, nombres de usuarios y contraseñas propias antes de que las aplicaciones sean activadas o se pongan a disposición de los clientes.

- Revisar el código antes de ponerlo en producción, a fin de identificar cualquier vulnerabilidad relacionada con la codificación.

Se deberá ejecutar igualmente un plan de pruebas para verificar que los cambios producidos por la instalación de parches de seguridad o actualización de aplicaciones de desarrollo propio, no alteran la seguridad del componente del sistema. También será preciso que todas las aplicaciones Web estén protegidas contra ataques conocidos mediante alguno de los siguientes mecanismos:

- Revisión de código en busca de vulnerabilidades manualmente o mediante una herramienta automatizada para la evaluación, como mínimo anualmente y después de cualquier cambio significativo.

- Instalación de un firewall de aplicación protegiendo las aplicaciones web, con las siguientes consideraciones:

  - Configuración de reglas que permitan la prevención y detección ataques WEB como Cross-site scripting (XSS), SQL injection y/o Denial-of Services (DoS).

  - Configuración y registro de logs de auditoría.

  - Validación de reglas mínimo semestralmente.

  - Actualización de acuerdo a los parches de seguridad publicados por los proveedores o según la publicación de nuevas vulnerabilidades.

11.2.15 MONITORIZACIÓN DE SISTEMAS DE INFORMACIÓN

El grado de monitorización necesario para los diferentes sistemas de información dependerá, en gran medida, de la tipología de información gestionada en cada caso por cada uno de los componentes de sistema, así como por el nivel de criticidad de los servicios funcionales a los que da soporte el sistema de información.

En este sentido, la posibilidad de llevar a cabo una investigación completa sobre determinada incidencia presentada puede requerir el análisis de la secuencia temporal de trazas o pistas de auditoría presentes en diferentes sistemas de información, para lo cual, es fundamental que los relojes asociados a los diferentes sistemas de procesamiento de información se encuentren sincronizados, siendo posible, en tal caso, explotar la información temporal aportada por el atributo fecha/hora de los distintos registros de actividad.

La premisa fundamental para poder plantearse la incorporación de estos registros de actividad es la existencia de una gestión de control de accesos incorporada al sistema de información o recurso de comunicación, esto es, de un mecanismo de identificación y autenticación de usuarios, así como la existencia de usuarios unívocos que permita la asignación de la autoría de los hechos (preservar el principio de responsabilidad), incluyendo aquellos usuarios con privilegios administrativos.

Los registros de actividad utilizados para el monitoreo de los sistemas de información, son aquellos que quedan almacenados en los logs descritos en los numerales 10.2 y 10.3 del Estándar PCI DSS.

Los lineamientos para la ejecución de las actividades de monitoreo se establecen en el procedimiento de Monitoreo de Seguridad de la Información (CIS176).

11.2.16 GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Anualmente o cuando existan cambios de alto impacto en la organización (Ejm: incorporación de nuevas tecnologías, inclusión/modificación/eliminación de procesos, reubicaciones físicas, entre otros) y/o nuevas ciberamenazas, se deberán identificar y controlar los riesgos que afecten la confidencialidad, integridad y/o disponibilidad de los datos de la organización clasificados como confidenciales y/o de uso interno, los cuales son descritos en el Instructivo Clasificación, Etiquetado y Protección de la Información (CIS104-IN004).

La metodología de riesgos de Seguridad de la Información debe estar orientada metodologías reconocidas en la industria (Ejm: Octave, Octave Allegro, Magerit, ISO

27005, ISO 31000, etc) y que sean capaces de identificar los activos de información (datos y sus contenedores), amenazas, vulnerabilidades y controles, de tal forma que se minimice cualquier riesgo que este fuera del apetito de riesgo de la organización.

El desarrollo de la gestión de riesgos de Seguridad de la Información estará alineado con la metodología de Riesgo Integral de Powerdata.

12 ANEXOS

- Estándar de Requerimientos de seguridad para aplicaciones (CIS211-AN05).
- Manual para la Gestión de Incidentes de Seguridad de la Información (CIS91-MA01).
- Anexo Políticas de Seguridad de la Información (CIS211-AN06).
- Guía de Seguridad de la Información (CIS211-AN07).
- Medidas De Seguridad Para Dispositivos Móviles (CIS211-AN15).
- Manual del Sistema de Gestión de Seguridad de la Información (CIS209-MA01).

13 GLOSARIO

Seguridad de la información: Es el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la entidad

Confidencialidad: Hace referencia a la protección de información cuya divulgación no está autorizada.

Integridad: La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.

Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

Ciberseguridad: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.

Ciberespacio: Entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.