POLÍTICA DE SEGURIDAD SODIGNATURE

1. OBJETIVO

Definir los lineamientos para fortalecer los controles de seguridad de la información que permiten la protección de la información de propiedad organizacional y la de carácter personal de los clientes, garantizando los principios de confidencialidad, integridad, disponibilidad.

2. ÁMBITO DE APLICACIÓN

El presente documento es de aplicación obligatoria para el personal que integra SODIG, conforme a los mecanismos y procedimientos establecidos por cada unidad organizacional en el ámbito de sus competencias, para el procesamiento y almacenamiento de la Información.

3. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

TÉRMINO	DEFINICIÓN
ACL	Access Control List
Activo de Información	Es todo elemento que contiene, transmite y procesa información, necesario para cumplir con la misión de SODIG, entre otros se encuentran: archivos y bases de datos; contratos y acuerdos; documentación del sistema, manuales de usuario, material de formación, aplicaciones, software del sistema, equipos informáticos y comunicaciones; servicios informáticos y de comunicaciones y las personas, que generan, transmiten y destruyen información.
Altos privilegios / Superusuario	Es el perfil de administrador de un ambiente informático, que tiene permisos para ejecutar tareas o acciones que un usuario normal no puede; tales como: cambiar el dueño o permisos de archivos e instalar sistemas operativos o bases de datos, modificar los archivos de configuración de los ambientes informáticos, etc.
Carácter especial	Es un símbolo que no forma parte del alfabeto ni tampoco de los números; tales como: @, -, _, ¡, ¿, |, etc.
Catastro de perfiles y roles	Listado de perfiles y roles que detalla los niveles de acceso que cada uno de ellos tendrá conforme a la taxonomía de servicios definida por la organización, contemplando conceptos de mínimo privilegio y segregación de funciones.
Confidencialidad	Conforme a la Norma ISO 27000 es la propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.
Datos maestros	Son un conjunto de información correspondiente a entidades como productos, clientes y proveedores, que no se modifican una vez que las transacciones se han completado.

Disponibilidad	Conforme a la Norma ISO 27000 es la propiedad de ser accesible y estar listo para su uso a demanda por una entidad autorizada.
Directorio Activo	Es una estructura jerárquica que almacena información acerca de los objetos existentes en la red y ponerlos a disposición de los administradores y los usuarios de la misma. La seguridad se integra con Active Directory a través de la autenticación de inicio de sesión y el control de acceso a los objetos del directorio.
Integridad	Conforme a la Norma ISO 27000 es la propiedad de exactitud y de completitud (cualidad de completo).
Infraestructura tecnológica	Se refiere a todas las tecnologías que interfieren y gestionan los procesos informativos y de comunicación de personas. Engloba el hardware y software que interviene en telecomunicaciones, automatización, comunicación de negocios y servicios de tecnologías de la información.
Infraestructura tecnológica base	Es la infraestructura tecnológica que está soportada sobre todo software base y de gestión.
Información agregada	Representa información de resumen, es decir no detallada.
Inventario	Lista ordenada de bienes valorables, con el detalle de sus características, que pertenecen a una persona, empresa o institución.
Metadata	Es la descripción clara de un dato que suele ser empleada como índice para localizar objetos de datos o documentos.
Mínimo privilegio	Consiste en reducir los privilegios de las cuentas de usuario al mínimo necesario para el desempeño de sus tareas autorizadas.
Mitigar	Es la reducción del impacto ante un riesgo materializado; la atenuación de los daños potenciales que puedan existir en un activo de información.
Perfil	Es la descripción clara del conjunto de capacidades y competencias que determinan la creación de un usuario para encarar responsablemente las funciones y tareas de una determinada actividad.
Pistas de auditoría	Consiste en una serie de archivos informáticos, y otros elementos de información que se examinan durante una auditoría, y muestran cómo las transacciones son manejadas por una empresa de principio a fin. Una pista de auditoría permite a un auditor rastrear los datos financieros relevantes llegando así al documento de origen (factura, recibo, bono, etc).
Responsable operativo	Es la persona encargada de ejecutar una operación asignada.
Información Reservada	Es aquella información pública expresamente establecida como reservada en leyes vigentes.
Rol	Un rol es una colección de permisos definida para todo el sistema que se pueden asignar a usuarios específicos. La combinación de roles definen la autorización de un usuario para hacer algo en algún sistema, y corresponden al nivel de compromiso de cada miembro de la organización para lograr la meta de preservar la información.
Sistemas de información	Aplicaciones, servicios, activos de tecnologías de la información y otros componentes para manejar la información.
Transacción crítica	Toda acción realizada dentro de un proceso que pueda recaer en una pérdida para SODIG o para los clientes.
Unidad Propietaria de la Información	Es la dependencia que es parte de los procesos sustantivos y adjetivos que realizan actividades esenciales para proveer y apoyar en el cumplimiento de la misión y objetivos estratégicos de SODIG, que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios y/o productos de procesamiento de información se clasifiquen, definan y revisen periódicamente las restricciones y accesos.

Usuario Interno	Es todo aquel personal que labora en SODIG, que tenga acceso de una manera u otra a los activos de información de SODIG.
Usuario Externo	Personal de instituciones públicas o privadas que teniendo relación con SODIG en cumplimiento de un convenio para el intercambio y uso de información o del objeto contractual respectivamente, llegan a tener acceso a los activos de información de SODIG.
Segregación de funciones	Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo. La asignación de funciones y sus respectivas responsabilidades garantizarán una adecuada segregación, evitando funciones incompatibles.

4. DESCRIPCIÓN NARRATIVA DE LA POLÍTICA

4.1. BASE LEGAL

Tabla 1 Normativa de la Política

NORMATIVA	ARTÍCULO
Código Orgánico Administrativo	Art. 24
Código Orgánico Integral Penal	Art. 179
Ley Orgánica del Sistema Nacional de Registro de Datos Públicos	Art. 4
Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos	Art. 9

4.2. LINEAMIENTOS GENERALES

Es potestad del responsable de cada una de las Unidades Organizacionales, actualizar y aprobar el contenido del documento de procesos denominado “Formatos” cuando lo considere necesario; previo a la comunicación formal del documento a los grupos de interés, se remitirá el Formato y/o anexo con los cambios realizados a la Unidad de Gestión de la Calidad para el respectivo análisis, en caso de que se hayan efectuado exclusivamente cambios de forma de un formato o anexo ya establecido, el responsable de procesos podrá continuar con la comunicación formal del documento; caso contrario se trabajará en conjunto con la Unidad de Gestión de la Calidad para analizar si existe impacto en la ejecución del proceso, lo cual generará una posible actualización de los Lineamientos, Manuales, Guías de Actividad o Instructivos a los cuales esté relacionado el “Formato” modificado.

Para la gestión de seguridad de la información, se deben aplicar las siguientes directrices:

4.2.1. LINEAMIENTOS DE MEDIOS LÓGICOS

a) Gestión de perfiles y roles

I. Las Unidades Propietarias de los aplicativos deben:
   1. Definir los perfiles y roles en cada uno de los aplicativos de su propiedad, considerando los privilegios con los que estos contarán, como, por ejemplo: transacción, consulta, impresión, etc.
   2. Levantar y mantener actualizado el catálogo de perfiles y roles de los aplicativos de su propiedad.
   3. Los perfiles y roles definidos deben permitir que exista una correcta segregación de funciones, evitando de esta manera la concentración de funciones en una sola persona y limitando la autorización de acceso solo la información indispensable para la ejecución de las labores asignadas.
   4. Como caso de excepción, si una dependencia no cuenta con el suficiente recurso humano para cumplir con la segregación de funciones, se debe realizar un análisis de pertinencia mismo que contará con la respectiva justificación previo al otorgamiento de los permisos; por lo que debe existir un comunicado por parte de la unidad de Talento Humano correspondiente, informando el número de personal que existe en la dependencia.
   5. Autorizar, restringir, delimitar el acceso y uso de la información a los usuarios, que de acuerdo con los perfiles, roles, responsabilidades y actividades requieran ingresar a consultar, registrar o actualizar parte o la totalidad de la información en los aplicativos informáticos de su propiedad; asegurando que los permisos concedidos se encuentren directamente relacionados con las funciones de cada usuario para el cumplimiento de sus actividades.
   6. Designar formalmente a los administradores de los sistemas de su propiedad, quienes se encargar de emitir los permisos que se hayan autorizado según el proceso vigente.

II. Unidad de Gestión de Tecnologías de la Información designara a los administradores de las herramientas tecnológicas de la plataforma base de SODIG, quienes serán los encargados de habilitar los accesos del personal.

III. Para la Infraestructura Tecnológica Base cada Responsable de la Unidad de Gestión de la Unidad de Gestión de Tecnologías de la Información al que pertenezca el usuario, aprobará la concesión o revocatoria de los permisos a los usuarios.

IV. La Unidad de Gestión de Seguridad de la Información debe:
   1. Definir los perfiles y roles de los usuarios que tengan acceso a la infraestructura tecnológica base de SODIG, considerando los privilegios con los que deben contar.
   2. Realizar control sobre la concesión o revocatoria de los permisos a los usuarios a la infraestructura tecnológica base de SODIG.
   3. Asegurar que sea posible identificar a cada persona que haya accedido a la infraestructura tecnológica base de SODIG, a través de un nombre de usuario personal.
   4. Asegurar que no existan cuentas genéricas salvo para el caso de ejecución de procesos automáticos. Para este caso, debe asegurar que hayan sido asignadas y registradas a personal de SODIG quien será responsable de la misma.
   5. Asegurar que se aplique el principio del mínimo privilegio para la asignación de permisos dentro de la infraestructura tecnológica base.

V. La Unidad de Gestión de Seguridad de la Información debe realizar revisiones periódicas sobre los permisos otorgados a la infraestructura tecnológica base y aplicativos de SODIG.

VI. La Unidad de Gestión de Talento Humano notificará a los administradores de los sistemas de SODIG, las desvinculaciones, y/o cambios administrativos que se

realicen con la finalidad de que los permisos otorgados en las herramientas tecnológicas tengan concordancia con el sistema de nómina de SODIG.

b) Contraseñas

1. El uso de la contraseña es de carácter personal e intransferible, por lo que no deben compartirse a terceras personas y serán conservadas de manera segura.
2. La Unidad de Gestión de Seguridad de la Información debe definir el método de hasheo de la contraseña, mismo que debe ser estándar en todos los aplicativos de SODIG.
3. Los usuarios de los sistemas de información son los encargados de registrar su contraseña, a través de métodos implementados en los aplicativos de SODIG, con la finalidad de que no intervengan terceras personas.
4. Los sistemas de información deben contar con métodos para que cada usuario sea quien registre su contraseña, en los casos de que el aplicativo no permita implementar este control se debe forzar al usuario a cambiar su clave la primera vez que ingresa al sistema, al no hacerlo el sistema debe negar el acceso.
5. La Unidad de Gestión de Tecnologías de la Información debe definir un mecanismo para la generación de clave, mientras que la Unidad de Gestión de Seguridad de la Información debe asegurar la implementación de este.
6. El acceso a la infraestructura base de SODIG no deben permitir la reutilización de las últimas 5 claves ingresadas.
7. Se debe implementar un segundo factor de autenticación en la infraestructura tecnológica base que permita esta configuración.
8. Los aplicativos internos de SODIG no deben permitir la reutilización de las últimas 5 claves ingresadas, así como para los aplicativos destinados para el uso de los clientes no debe permitir la reutilización de las últimas 3 claves; tampoco debe permitir el registro de fechas de nacimiento y/o sus nombres.
9. Para los aplicativos desarrollados por SODIG en los que se requiera credenciales, los usuarios internos y externos deben seguir el estándar de seguridad para la selección de sus contraseñas, evitando así accesos no autorizados, como se muestra a continuación:

Tabla 2 Formato de seguridad para caracteres

	Longitud mínima	Longitud máxima	Letras Mayúsculas	Caracteres especiales	Letras Minúsculas	Números	Medidor Control de fortaleza
Usuario interno / Usuario externo	10 caracteres	50 caracteres	✓	1 carácter	✓	✓	

10. Se debe impedir el uso de repeticiones de caracteres o patrones o secuencias obvias, como, por ejemplo: abcd, qazwsx, asdf, 23456, etc.
11. La Unidad de Gestión de Seguridad de la Información debe verificar que los desarrollos informáticos de acceso realizados en SODIG, cuenten con un medidor de fortaleza de la contraseña, que cumpla las políticas de contraseña segura de SODIG.
12. La Unidad de Gestión de Tecnologías de la Información debe definir y diseñar un mecanismo que mida el nivel de fortaleza de la clave que valide las condiciones de los literales 8, 9, 10; este debe alertar al usuario cuando la clave registrada es débil, moderada o alta. Dicho mecanismo debe ser implementado en todo software desarrollado por SODIG.
13. Las contraseñas serán almacenadas de manera cifrada en las bases de datos y/o en los archivos de parametrización en caso de ser necesario.

14. El software desarrollado por SODIG debe implementar los controles necesarios, a fin de que se impida que el navegador web recuerde la contraseña de los usuarios.
15. Para el software destinado para uso operativo de SODIG se establecerá un periodo de vigencia de la clave de 60 días, posterior a ello se debe obligar a cambiar su contraseña de acceso y en caso de no hacerlo se restringe el mismo. Para los aplicativos que no se pueda implementar éste control, la Unidad de Gestión de Tecnologías de la Información deberá emitir un informe técnico con la justificación.
16. Para los usuarios externos se establece que en todos los aplicativos de SODIG la vigencia de la clave sea de 1 año, posterior a ello se debe obligar a cambiar su clave y en caso de no hacerlo se restringe el acceso, sin que esto conlleve a una inactivación de los permisos.
17. La Unidad de Gestión de Seguridad de la Información, debe generar las contraseñas de administradores con privilegios de superusuario de la infraestructura tecnológica base de SODIG, misma que debe ser entregada en sobre cerrado al Responsable de la Unidad de Gestión de Tecnologías de la Información, para el custodio.
18. Las contraseñas de usuarios administradores con privilegio de superusuario de la infraestructura tecnológica base de SODIG, deben ser cambiadas al menos una vez al año.
19. Todo software desarrollado por SODIG debe bloquear el acceso si ha existido 3 intentos consecutivos de ingresos fallidos, mismos que deben ser inicializados cuando exista un ingreso al sistema exitoso, se debe notificar de este bloqueo al correo electrónico del usuario interno, externo.
20. Todo software desarrollado por SODIG debe contar con un proceso de recuperación de contraseña y desbloqueo de contraseña que contemple métodos de autenticación de doble factor (“algo que sabe”, “algo que tiene” y dentro de lo posible “algo que es”). Se bloqueará definitivamente al usuario si la recuperación de contraseña no es exitosa luego de 3 intentos fallidos, por lo que debe realizar el proceso de desbloqueo de manera presencial.

c) Control de acceso y autenticación

I. La Unidad de Gestión de Tecnologías de la Información debe asegurar que todo software desarrollado por SODIG, ya sean web o móviles de uso de clientes, usuario interno y usuario externo cumplan con las siguientes condiciones de seguridad en ambientes de producción:
    1. Cuente con doble factor de autenticación (“algo que sabe”, “algo que tiene” y dentro de lo posible “algo que es”) para el ingreso a los sistemas.
    2. Implementar mecanismos de autenticación al inicio de sesión de los clientes, en donde el nombre de usuario debe ser distinto al número de cédula de identidad.
    3. Cuente con un método de alertas para notificar a los usuarios externos cuando se registre un acceso exitoso o fallido, mediante un medio de comunicación que SODIG defina como oficial, como: por correo electrónico o mensajes de texto. Las notificaciones se deben almacenar en un registro histórico y el correo debe indicar por lo menos la siguiente información:
        - Identificación del usuario interno única;
        - Identificación de usuario externo única;
        - Dirección IP desde donde se realizó el intento de ingreso al sistema;
        - País de procedencia de la IP;
        - Fecha y hora en formato dd/mm/aaaa hh:mm:ss;
        - Módulo o servicio en el que se realizó el intento de ingreso al sistema;
        - Novedad: ingreso exitoso o fallido.
    4. Las sesiones de todos los aplicativos de SODIG tendrán un tiempo de duración por inactividad en el aplicativo, luego del cual se deberá cerrar la sesión y solicitar que la persona vuelva a realizar el proceso de autenticación, conforme al siguiente cuadro:

Tabla 3 Destino de uso de la aplicación

Destino de uso de la aplicación	Tiempo de duración de sesión por inactividad
Unidades de Gestión de SODIG	5 minutos
Clientes Externos	20 minutos
Controlador de dominio	3 minutos
Personal rotativo de monitoreo y atención al cliente	Según jornada laboral

5. Inactivar las credenciales concedidos a los usuarios internos y externos, si estos no han hecho uso de sus credenciales en el lapso de 30 días calendario. Luego de lo cual deben solicitar nuevamente el acceso conforme al proceso vigente para concesión de credenciales.
6. Dentro de lo técnicamente posible, el software de SODIG debe estar integrado al sistema de nómina de SODIG, con la finalidad de que se desactiven automáticamente los permisos concedidos a los servidores de SODIG, cuando estos hayan culminado su relación laboral con SODIG, se encuentren en goce de sus vacaciones, licencia por maternidad, cambio administrativo. Se restituirán los permisos automáticamente cuando haya culminado la fecha de retorno para los siguientes casos: vacaciones y licencia por maternidad.
7. Para la confirmación de transacciones críticas se debe implementar un método de autenticación diferente a usuario y contraseña, pudiendo ser esto: código OTP, reconocimiento facial, etc. Se debe enviar una notificación al usuario de la transacción ejecutada, sea correcta o un intento.
8. Al utilizar la validación por código OTP debe cumplir el siguiente estándar:
   - Compuesto por 6 dígitos.
   - Envío del código OTP al correo electrónico y/o al número de celular registrado.
   - Tiempo de vigencia del código será definido conforme a la capacidad de la infraestructura tecnológica de SODIG.
   - Luego de tres (3) intentos consecutivos fallidos de registro del código OTP se procederá a un bloqueo temporal de 20 minutos.
9. Si se bloqueó temporalmente el acceso por 3 veces seguidas (9 en total), se realizará un bloqueo definitivo de la cuenta de usuario interno o externo, según sea el caso.
10. Notificación del bloqueo al correo electrónico y/o al número de celular registrado por el usuario interno o externo. Mensaje de número de intentos fallidos acumulados en el propio sistema.
11. Notificación por correo electrónico de alertas a los usuarios externos cuando se ejecuten transacciones críticas o realicen actividades y/o eventos anómalos en los sistemas o aplicativos de SODIG, de igual manera se debe notificar a los responsables operativos.

II. La Unidad de Gestión de Tecnologías de la Información debe asegurar que en ambientes de producción:
   1. Las cuentas con altos privilegios (superusuario) o cuentas genéricas de esquemas de bases de datos o sistemas, no deberán ser utilizadas para las tareas de administración o monitoreo diario, sino únicamente en casos excepcionales o emergentes, con un proceso y mecanismo de control de uso de estas, el cual se encontrará bajo la responsabilidad además de ser controlado por la Unidad de Gestión de Seguridad de la Información.
   2. Todas las estaciones tecnológicas de trabajo deben estar asociadas a un controlador de dominio de SODIG, acorde a su estándar de identificación único

que debe ser definido por la Unidad de Gestión de Tecnologías de la Información.

3. Implementar y mantener actualizado soluciones de antivirus y antimalware para la protección de la red interna de SODIG.

III. En ambientes de producción la Unidad de Gestión de Seguridad de la Información debe:

1. Establecer las directrices de configuración, generación, custodia y actualización de contraseñas de usuarios con altos privilegios, en la infraestructura tecnológica base de SODIG.
2. Controlar y monitorear el uso de los permisos concedidos para el acceso a la infraestructura tecnológica base de SODIG, a fin de detectar actividades no autorizadas y eventos anómalos.
3. Emitir un informe mensual de novedades del control realizado sobre los accesos a la infraestructura tecnológica base de SODIG.
4. Controlar los accesos locales y/o remotos de todos los usuarios internos o externos, a la infraestructura tecnológica base de SODIG.
5. Elaborar una directriz que permita controlar las acciones ejecutadas dentro de lo que permita el rol o perfil asignado al usuario con permisos privilegiados dentro de la infraestructura tecnológica base.
6. Elaborar y mantener actualizado una bitácora de la asignación de los usuarios privilegiados dentro de la infraestructura tecnológica base de SODIG.
7. Asegurar que en cada aplicativo se ejecuten únicamente los puertos de red, protocolos y servicios que se requieran para su operación y administración técnica, en ambientes de producción.
8. Asegurar que se realicen escaneos periódicos de puertos en todos los aplicativos y que se advierta a la Unidad de Gestión de Tecnologías de la Información, si se detectan puertos no autorizados en un aplicativo para que toma las acciones pertinentes.
9. Los usuarios externos, al conectarse a la red de SODIG contarán con accesos mínimos relacionados con las actividades que vayan a realizar y se debe guardar la trazabilidad del acceso de los usuarios.

IV. La Unidad de Gestión de Seguridad de la Información debe:

1. Realizar revisiones periódicas sobre los derechos concedidos a los usuarios de la información.
2. Analizar y evaluar los reportes del control del uso de los servicios tecnológicos de SODIG para detectar actividades no autorizadas, con la finalidad de tomar las acciones pertinentes según sea el caso.
3. Revisar periódicamente las acciones y eventos anómalos realizados por los usuarios administradores funcionales y técnicos de los aplicativos.
4. Elaborar y proponer recomendaciones para minimizar brechas de seguridad de la información, identificadas sobre el control de accesos de los sistemas.

V. Las Unidades Propietarias de la Información deben establecer e implementar el plan de acción para mitigar las vulnerabilidades encontradas en los sistemas de su responsabilidad, recomendadas por la Unidad de Gestión de Seguridad de la Información y/o la Unidad de Gestión de Tecnologías de la Información. Sobre el avance de la implementación del plan, las Unidades de Negocio deben reportar a la Unidad de Gestión de Seguridad de la Información.

VI. Las redes de comunicación de SODIG deben contar con métodos de autenticación que eviten y detecten accesos no autorizados.

d) Registros y pistas de auditoría en ambientes productivos

I. Las Unidades Organizacionales de los procesos sustantivos en coordinación de la Unidad de Gestión de Seguridad de la Información y de la Unidad de Gestión de Seguridad de la Información, identificarán las transacciones críticas en sus aplicativos, tanto en ambientes de producción, como aquellos que se encuentren en proyecto de desarrollo, en los que se implementarán las pistas de auditoría y

métodos de alerta, así como también notificaciones de acciones y eventos anómalos.

II. La Unidad de Gestión de Seguridad de la Información debe:
   a. En coordinación de las unidades que conforman la Unidad de Gestión de Tecnologías de la Información, emitir el lineamiento de seguridad de logs y pistas de auditoría en SODIG, que cubra la totalidad de aplicativos, herramientas informáticas y accesos a la infraestructura tecnológica base de SODIG.
   b. Implementar en coordinación de la Unidad de Gestión de Tecnologías de la Información, un sistema de gestión de información de seguridad y eventos (Security Information and Event Management - SIEM) o una herramienta que permita el análisis de registros de pistas de auditoría para la correlación de estos y emita alertas de eventos anómalos.
   c. Realizar un control periódico sobre los logs de la infraestructura tecnológica base de SODIG, con la finalidad de identificar actividades no autorizadas y emitirá un informe del control realizado a la Unidad de Gestión de Seguridad de la Información.

III. La Unidad de Gestión de Tecnologías de la Información debe definir el mecanismo para que todos los aplicativos desarrollados y/o adquiridos por SODIG, cuenten con pistas de auditoría que permitan la trazabilidad de los eventos en las transacciones críticas identificadas, como acceso, registro, eliminación y/o modificación de la información.

IV. La Unidad de Gestión de Tecnologías de la Información debe asegurar que:
   1. La fecha y hora de todos los servidores y dispositivos de red se encuentren sincronizados para que las marcas de tiempo en los registros sean consistentes.
   2. La infraestructura tecnológica base que almacena logs y pistas de auditoría cuente con el espacio de almacenamiento adecuado para los registros generados en base al análisis de capacidades correspondiente, conforme lo definido en el procedimiento de seguridad de logs y pistas de auditoría en SODIG.
   3. Activar los logs que permitan la trazabilidad de los cambios realizados en los sistemas operativos y bases de datos que almacenen información crítica.

V. La Unidad de Gestión de Seguridad de la Información debe realizar una revisión periódico o bajo demanda, sobre los registros de pistas de auditoría de las transacciones críticas identificadas.

e) Cifrado

I. La Unidad de Gestión de Tecnologías de la Información debe definir los controles criptográficos para la protección de contraseñas de acceso a los aplicativos desarrollados por o para SODIG; mientras que la Unidad de Gestión de Seguridad de la Información debe asegurar que dichos controles sean aplicados. Estos controles serán considerados como reservados.

II. La Unidad de Gestión de Seguridad de la Información debe:
   a. Definir los algoritmos de cifrado (encriptación) que se utilizarán en toda SODIG, dependiendo del tipo de control a aplicar, el propósito y el proceso del negocio. Esta definición se revisará periódicamente y actualizará de ser necesario.
   b. Establecer los mecanismos de verificación de integridad de información, por ejemplo, mediante herramientas que permitan obtener el código hash de la información o de archivos, considerando las buenas prácticas de seguridad informática.
   c. Asegurar que el almacenamiento, transferencia y/o transmisión de la información digital clasificada como confidencial y reservada, cumplan los mecanismos de cifrado definidos.

III. Los canales de datos de la red externa deben ser cifrados punto a punto conforme a los lineamientos y estándares técnicos definidos por la Unidad de Gestión de Seguridad de la Información.

IV. En los casos en los que exista solicitudes de organismos de control u órdenes judiciales, la información cifrada puede ser puesta a disposición en forma no cifrada previa autorización de la Unidad Propietaria de la Información.

V. La información en soluciones móviles debe ser cifrada conforme a las definiciones establecidas por la Unidad de Gestión de Seguridad de la Información.

f) Adquisición, desarrollo y mantenimiento de sistemas de información

I. Las Unidades Propietarias de los aplicativos deben:
   1. Solicitar, validar y aprobar los requerimientos funcionales de los sistemas de información de su propiedad.
   2. Los registros que son almacenados en la base de datos del aplicativo, deben cumplir las validaciones y reglas de negocio.
   3. En coordinación de la Unidad de Gestión de Seguridad de la Información identificar la información crítica y solicitar su encriptación y/o enmascaramiento a la Unidad de Gestión de Tecnologías de la Información.
   4. Elaborar y mantener actualizados los manuales de usuario de los aplicativos de su propiedad o contratados, en coordinación de la Unidad de Gestión de Tecnologías de la Información.
   5. Describir la metadata contenida en los sistemas de información de su propiedad.

II. Las unidades que conforman SODIG no podrán hacer uso de software que no haya sido autorizado por la Unidad de Gestión de Tecnologías de la Información, dentro de la normativa vigente.

III. La Unidad de Gestión de Tecnologías de la Información debe:
   a. Realizar el análisis de impacto técnico del desarrollo o mantenimiento solicitado por la Unidad Propietaria del aplicativo, considerando el software y hardware involucrado.
   b. Implementar controles de seguridad informáticos con la finalidad de que no quede expuesta información sensible o código fuente en los casos que se presente un error del aplicativo (control de excepciones o errores en los sistemas de información).
   c. Verificar los controles de seguridad aplicados y realizar análisis de vulnerabilidades de seguridad informática a todos los aplicativos previo al paso a producción y en ambientes de producción.
   d. Elaborar y mantener actualizados los manuales técnicos (documentación de desarrollo, diccionarios de datos, modelos conceptual y lógico de la base de datos, entre otros) de todos los aplicativos desarrollados por SODIG y asegurar que existan manuales técnicos de todo sistema que haya sido desarrollado a medida para SODIG.
   e. Asegurar que en los procesos de adquisición de sistemas y software para SODIG, se entreguen como mínimo los manuales de implementación que permitan a SODIG instalar, configurar y parametrizar el software adquirido, así como también, los manuales de usuario.
   f. Asegurar que se entregue la arquitectura de la solución, los manuales técnicos de instalación, configuración, soporte y operación; así como de usuario, los cuales serán difundidos, publicados y actualizados de forma permanente conforme a los lineamientos de la Unidad de Gestión de Tecnologías de la Información.
   g. Para los casos de migración de información en coordinación de las unidades involucradas, debe determinar y aplicar controles técnicos para garantizar la integridad, disponibilidad y confidencialidad de la información.

h. Identificar los datos maestros para evitar duplicidad de información que es de uso transversal en los aplicativos.
i. Establecer ambientes aislados con la debida segregación de accesos para desarrollo, pre-producción y producción, los cuales deben contar con la capacidad y seguridad requeridas para cumplir sus objetivos.
j. Gestionar la verificación del código fuente de los componentes de software desarrollados por SODIG para evitar el paso a producción de código que no cumpla el estándar definido en SODIG.
k. Establecer un control de cambios en los aplicativos y documentación, que debe contar con la aprobación de la Unidad Propietaria de la Información.
l. En coordinación con los propietarios de la información se deben realizar las pruebas para garantizar que el aplicativo ejecute las funciones requeridas, que la funcionalidad y el desempeño de otros aplicativos e información existentes no se vean afectadas por el cambio, que no se hayan degradado la confidencialidad, integridad y disponibilidad de la información debido al cambio; y, que se encuentre con toda la documentación técnica y funcional actualizada; una vez concluidas exitosamente las pruebas, se debe registrar la aprobación del cambio en conjunto.
m. En coordinación con las unidades de negocio y de apoyo, se definirá el software autorizado para uso dentro de SODIG conforme a sus necesidades y removerá el no autorizado.
n. Solicitar el registro de la propiedad intelectual a favor de SODIG de los aplicativos que hayan sido desarrollados o contratados con terceros para desarrollo de software.

g) Actualizaciones a la información a través de base de datos

I. Las Unidades Propietarias de los aplicativos deben:
1. Solicitar que la actualización de la información y datos se realicen únicamente a través de sistemas de información de SODIG, y en casos excepcionales, la actualización se realizará directamente a la base de datos, previa solicitud y autorización, y hasta que se implementen los desarrollos necesarios para cubrir estas necesidades.
2. En los casos de no contar con sistemas de información que permitan la actualización de datos, se debe solicitar y aprobar las afectaciones directas a la base de datos considerando el impacto que esta pueda causar a otras unidades de negocio, a través del documento de actualización definido por la Unidad de Gestión de Tecnologías de la Información. Una vez realizados los cambios debe asegurar que estos hayan sido realizados bajo los criterios establecidos en el pedido de actualización.
3. La Unidad de Gestión de Tecnologías de la Información debe llevar un registro del motivo, quienes solicitan, autorizan y ejecutan la solicitud de actualización de la información.

h) Control de Hardware y Software

a. La Unidad de Gestión Administrativa Financiera debe:
- Establecer el lineamiento de gestión de activos.
- Definir las directrices de etiquetado y manejo de activos, estableciendo las responsabilidades del custodio.
- Elaborar el procedimiento de asignación, traslado y baja de activos.
- Asegurar que todo custodio de los activos cuente con un acta de entrega recepción del bien.
- Asegurar que todo bien cuente con un custodio designado.
- En coordinación con las unidades especializadas, clasificar e inventariar los bienes que conforman la infraestructura tecnológica de SODIG.

b. La Unidad de Gestión de Tecnologías de la Información, en relación a la infraestructura tecnológica de SODIG, debe definir un lineamiento de gestión de hardware y software que permita:
   - Asegurar que los equipos de hardware cuenten con soporte y mantenimiento técnico.
   - Asegurar que el software cuente con las licencias o suscripciones de uso.
   - Asegurar la aplicación de los parches de seguridad actualizados de las versiones de software utilizadas.

c. La Unidad de Gestión de Tecnologías de la Información debe utilizar herramientas de detección de software y hardware, que sirva de base para inventariar todos los recursos físicos y lógicos de la infraestructura tecnológica de centros de datos y estaciones de trabajo.

d. Los custodios de los activos deben evitar daños en los códigos o etiquetas que permiten la identificación de los activos.

e. La Unidad de Gestión de Seguridad de la Información debe validar que se implementen mecanismos de control que eviten la instalación de software no autorizado.

i) Seguridad perimetral y de infraestructura base

I. La Unidad de Gestión de Seguridad de la Información, debe:
   1. Definir los lineamientos y/o directrices de seguridad informática para todos los dispositivos de red local.
   2. Implementar herramientas para la detección y control de vulnerabilidades que alerten oportunamente a los administradores de red para que se realicen las acciones de mitigación correspondiente.
   3. Realizar periódicamente o bajo demanda escaneos, manuales o automáticos, de vulnerabilidades a la red e infraestructura tecnológica de SODIG.
   4. Solicitar a la Unidad de Gestión de Tecnologías de la Información que realicen la mitigación de las vulnerabilidades descubiertas.
   5. Comparar periódicamente los resultados de escaneos de vulnerabilidades consecutivos para verificar que estas se hayan mitigado de manera oportuna.
   6. Definir y mantener la directriz de seguridad informática para todos los sistemas operativos y software autorizados.
   7. Activar y monitorear la colección de paquetes de datos que circulen por el perímetro interno y externo de los servicios o aplicativos internos o de clientes.
   8. Definir y utilizar herramientas para escanear automáticamente todos los sistemas en la red de forma mensual o más frecuente para identificar todas las vulnerabilidades potenciales en los sistemas de SODIG.
   9. Identificar y asociar los puertos y protocolos activos de la infraestructura tecnológica base de tal manera que se asegure que en cada sistema se ejecuten solo los puertos de red y los protocolos que se requieran con fines de negocio y administración técnica.
   10. Estandarizar firewalls de aplicaciones (WAF) frente a servidores críticos para verificar y validar el tráfico que va al servidor. Cualquier evento no autorizado debe ser bloqueado y registrado.
   11. Definir y mantener la configuración de seguridad estandarizada y documentada para todos los equipos de red autorizados.
   12. Documentar todas las reglas de configuración que permiten que el tráfico fluya a través de dispositivos de red, donde se debe registrar el motivo específico para cada regla, el nombre del responsable de esa necesidad de negocio y la duración esperada de la necesidad.
   13. Comprobar periódicamente que se encuentren instaladas la última versión estable de cualquier actualización de seguridad en todos los equipos de red.
   14. Denegar las comunicaciones con direcciones IP de Internet maliciosas conocidas o no utilizadas y limitar el acceso solo a los intervalos de

direcciones IP confiables y necesarios en cada uno de los límites de la red de la organización.

15. Implementar una política restrictiva en el perímetro para denegar la comunicación sobre los puertos TCP o UDP no autorizados.
16. Implementar sensores de sistemas de detección y prevención de intrusos (IDS/IPS) basados en red para buscar, detectar y bloquear ataques en base a comportamiento inusual en la red.
17. Implementar mecanismos de Prevención de Perdida de Datos - DLP en la infraestructura informática de SODIG.
18. Evidenciar que cada una de las directrices de seguridad informática se haya aplicado sobre el equipamiento tecnológico relacionado a seguridad perimetral.

II. La Unidad de Gestión de Tecnologías de la Información debe:

1. Implementar herramientas de actualización de software para garantizar que los sistemas operativos en los servidores y equipos de estaciones de trabajo cuenten con las actualizaciones de seguridad más recientes de las versiones de software utilizadas, provistas por el fabricante.
2. Implementar firewalls de aplicaciones (WAF) frente a servidores críticos para verificar y controlar el tráfico que va al servidor.
3. Mantener imágenes o plantillas de las configuraciones y sistemas operativos de la infraestructura base de la organización para utilizarlas como insumo en la ejecución de los planes de contingencia.
4. Almacenar las imágenes de la configuración de servidores de forma segura; se debe utilizar los lineamientos definidos por la Unidad de Gestión de Seguridad de la Información.
5. Utilizar al menos dos fuentes de tiempo sincronizadas para asegurar que la fecha y hora de los servidores y estaciones de trabajo se encuentren sincronizadas.
6. Instalar la versión actualizada estable de seguridad en todos los equipos de red considerando las versiones de software utilizadas.
7. Mantener los equipos de red con métodos de autenticación seguros, definidos por la Unidad de Gestión de Seguridad de la Información.
8. Administrar la infraestructura de red mediante VLANs separadas y ACLs.
9. Asegurar que todo el tráfico de red hacia o desde Internet pase a través de un proxy de capa de aplicación que esté configurado para filtrar conexiones no autorizadas.

j) Correo electrónico

I. La Unidad de Gestión de Seguridad de la Información debe definir los tipos de archivos permitidos para que sean enviados y recibidos como documentos adjuntos a un correo electrónico.

II. La Unidad de Gestión de Seguridad de la Información debe asegurar que los tipos de archivos permitidos sean enviados y recibidos como documentos de adjuntos a un correo electrónico, así como la restricción de los tipos de archivos no permitidos.

III. La Unidad de Gestión de Tecnologías de la Información debe definir el cliente de correo electrónico de SODIG autorizado.

IV. La Unidad de Gestión de Tecnologías de la Información debe:

1. Implementar mecanismos para detectar y desinstalar o deshabilitar cualquier plugin o aplicación add-on para navegador o cliente de correo electrónico no autorizados.
2. Limitar y controlar el uso de lenguajes de scripting en el servicio de correo electrónico de SODIG.

3. Bloquear todos los archivos adjuntos de correo electrónico que no sean definidos por SODIG.
4. Utilizar técnicas y tecnología que permita analizar y bloquear los archivos adjuntos de correo electrónico que tengan un comportamiento malicioso.
5. Implementar los estándares Sender Policy Framework (SPF), para prevenir que los creadores de spam envíen mensajes con los dominios registrados de SODIG.
6. Implementar los estándares DomainKeys Identified Mail (DKIM), para asegurar el no repudio de los mensajes emitidos a través de los dominios registrados por cualquier dependencia de SODIG.
7. Asegurar que el correo electrónico de SODIG cuente con un antivirus y antimalware actualizado.
8. Asegurar que el correo electrónico de SODIG cuente con un control anti-spam con, al menos, un banco de listas negras.

k) Internet

La Unidad de Gestión de Seguridad de la Información debe:

a. Definir las reglas de uso del internet a nivel de SODIG, estableciendo perfiles de usuario, accesos de navegación restringidos y de libre navegación, y los horarios de uso.
b. Monitorear el uso de internet en base a las reglas definidas.
c. Debe implementar una solución para el filtrado URL a nivel de SODIG que mantenga una actualización y sincronización de definiciones de sitios web.
d. Limitar el acceso a los servicios de almacenamiento en la nube, así como también a los servicios de transferencia de datos a aquellos autorizados por los procesos gobernantes.
e. Utilizar servicios de filtrado de DNS para ayudar a bloquear el acceso a dominios maliciosos conocidos.

l) Control de escritorios, pantallas, equipos e información del usuario

1. Fuera de horarios laborables, El personal deben dejar la información confidencial protegida bajo cualquier mecanismo pudiendo ser: bajo llave en archivadores, muebles o caja fuerte que se haya destinado para estos fines, siempre pensando en la confidencialidad y reserva de la información, esto incluye los documentos impresos, CD's o cualquier medio removible aprobado por SODIG.
2. Se prohíbe la reutilización de hojas impresas que contengan información considerada y/o clasificada como confidencial o reservada, debiendo esta ser destruida mediante máquina trituradora de papel.
3. Todas las estaciones de trabajo deben usar el papel tapiz y el protector de pantalla definido por la Unidad de Gestión de Comunicación Social de SODIG, el cual se activará automáticamente después de tres (3) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.
4. Los funcionarios deben bloquear su computador mediante un secuencia de teclas (control + alt + suprimir, símbolo de Windows + L, etc.), como medida de seguridad cada vez que se retiren de su sitio de trabajo, el cual solo se podrá desbloquear con la contraseña del usuario.
5. No deben quedar a la vista ningún tipo de información considerada sensible y relacionada con SODIG, tales como: nombres de usuarios, contraseñas, Direcciones IP, directorios, contratos, información de clientes, datos personales de colaboradores, entre otros; en cuadernos, pizarras, post-it's, o cualquier mecanismo impreso de acceso visual.
6. Las estaciones de trabajo deben ser apagadas al final de la jornada laboral o al finalizar una sesión de trabajo, exceptuando las que se encuentren ejecutando

procesos posteriores al horario de la jornada laboral, o se encuentren en modalidad de teletrabajo.

7. Todo computador portátil debe permanecer con un candado de seguridad todo el tiempo, asegurándose que el candado esté correctamente instalado y que la contraseña y/o llave de este no quede expuesta.
8. Los puertos USB del computador deben ser restringidos para el uso de cualquier tipo de almacenamiento masivo, incluido dispositivos telefónicos móviles. Únicamente se permitirá su uso con la previa autorización del responsable de la unidad a la que pertenece la persona y con su debida justificación.
9. La Unidad de Gestión de Seguridad de la Información debe efectuar inspecciones periódicas (mínimo una vez al año) o según su criterio para evaluar la efectividad del control que consta en el presente lineamiento.

4.2.2.LINEAMIENTOS DE ENTREGA DE INFORMACIÓN

a) Normas generales para la entrega de información

1. La atención y respuesta de solicitudes de información presentados por los agentes fiscales, juzgados, cortes y tribunales de ámbitos cantonal, provincial y regional deben ser atendidos por las Unidades Organizacionales dentro de su ámbito de acción, teniendo en cuenta los plazos y términos de atención establecidos en la Ley o por el organismo requirente. Para efectos de elaboración de reportes, informes o gestión de control, esta tarea se ejecutará exclusivamente por el responsable de las áreas o unidades funcionales competentes.
2. Las solicitudes de información realizadas por orden judicial deben ser procesados y atendidos dentro de los plazos establecidos por dichas instituciones.
3. La facultad de los órganos de control para solicitar y requerir información a SODIG debe estar definida conforme lo manda el entorno constitucional y legal que los regulan.
4. Si la información solicitada es para un tercero y no para la persona dueña de la información o para un Juez, Fiscal, Organismo de Control o Auditoría Interna, la dependencia que haya recibido inicialmente la solicitud de información debe contestar al solicitante la Negación de entrega de información.
5. En caso de que la solicitud de información no corresponde atender al área direccionada, debe ser redireccionado inmediatamente a la dependencia competente, con la finalidad de que la atención del requerimiento sea realizada dentro de los plazos establecidos.

b) Acceso a información entre Unidades Propietarias de la Información de SODIG

1. Cada Unidad Propietaria de la Información que requiera tener acceso a información que le pertenezca a otra, debe solicitar la respectiva autorización a la Unidad correspondiente.
2. La Unidad Propietaria de la Información no podrá autorizar más información de la que sea estrictamente necesaria para el correcto desempeño de las funciones que se realizarán conforme a la solicitud presentada por la otra Unidad, por lo que deberá garantizar la confidencialidad, integridad y disponibilidad de la información.
3. El mecanismo para el acceso a la información debe ser definido por la Unidad de Gestión de Tecnologías de la Información.

4.2.3.LINEAMIENTOS DE MEDIOS FÍSICOS

a) Seguridad de documentación física

1. Toda dependencia de SODIG es el custodio de la información que sea generada en su unidad, por lo cual son responsables de asegurar la integridad, disponibilidad y la confidencialidad o reserva de la información.
2. No se permite que la documentación que contenga información catalogada como confidencial y/o reservada, se encuentre en lugares de libre acceso para personas no autorizadas; para lo cual, esta información siempre debe tener asignado un custodio, quien llevará un registro del uso de la documentación.
3. Al final de la jornada de trabajo el personal de SODIG tiene la obligación de guardar la información que se encuentre bajo su custodia en lugares seguros, tales como: archivadores con llave, bóvedas de seguridad, etc.
4. Se debe contar con un Responsable de Archivo quien debe ser designado por la Gerencia General o la Unidad de Gestión Administrativa Financiera.
5. Todos los archivos activos y pasivos, independientemente del nivel de consulta, deben estar organizados.
6. No se permitirá el acceso a los archivos de SODIG (activos y pasivos), sin la autorización del responsable de la Unidad de Gestión y sin la presencia del responsable del archivo.
7. El Responsable de Archivo debe llevar una bitácora de acceso al mismo, con la siguiente información:

    - Fecha y hora de acceso;
    - Cédula de identidad de la persona que ingresa al archivo;
    - Nombres completos de la persona que ingresa al archivo;
    - Motivo;
    - Código de la carpeta que fue revisada;

8. Todo archivo ya sea activo, intermedio, central o histórico debe contar con las medidas de seguridad tales como: cámaras de seguridad, equipo de detección de humo, sistema de adecuación ambiental y equipamiento contra incendios.

b) Gestión de acceso físico

1. Las áreas de circulación en todas las dependencias de SODIG serán clasificadas dentro de los siguientes tipos de acceso acorde a su circulación:
    - Áreas de libre circulación o no restringidas, serán las áreas donde se encuentren clientes, proveedores y visitantes en general, en espera de la autorización correspondiente para el ingreso a las diferentes unidades administrativas o técnicas de SODIG.
    - Áreas de Circulación Interna, serán las áreas internas de cada Unidad de Gestión destinadas para el uso del personal que labora en SODIG y/o clientes, proveedores y visitantes en general que cuenten con el permiso necesario para el ingreso.
    - Áreas Restringidas, serán aquellas donde se ubican, procesan o almacenan información de suma importancia para SODIG.
2. No se permitirá el acceso de personal no autorizado en áreas restringidas de SODIG.
3. A las áreas restringidas se prohíbe el ingreso de equipos fotográficos, de vídeo, audio u otro tipo de dispositivo informático, salvo excepciones expresamente autorizadas por el responsable o autoridad del área.
4. El personal de SODIG debe portar una credencial, que permita identificarlos y diferenciarlos dentro de las diferentes instalaciones de SODIG, controlando el acceso a las áreas restringidas. Para lo cual la Unidad de Gestión de Talento Humano debe dotar de las credenciales a todo el personal que labora en SODIG, mientras que la Unidad de Gestión Administrativa Financiera será la

responsable de asegurar que todas las dependencias de SODIG cuenten con credenciales para los visitantes al SODIG, quienes emitirán las directrices técnicas para su implementación en toda SODIG.

5. Se debe contar con un control de visitas para registrar el acceso físico a las instalaciones de SODIG, entregando a los visitantes credenciales de identificación que permitan diferenciar el acceso al que se le ha autorizado (libre circulación, circulación interna y circulación restringida). El ingreso en áreas definidas como restringidas de terceros autorizados, debe efectuarse con el acompañamiento de personal autorizado. Toda visita a las áreas restringidas debe ser registrada en bitácoras, identificando al personal que ingresa y el motivo de su visita.
6. Se define a áreas restringidas todas aquellas en donde se almacene, genere y/o procese información, tales como:
    - Archivos que alberguen información confidencial y/o reservada.
    - Centro de Cómputo y áreas de almacenamiento de respaldos de información.
    - Oficinas de SODIG que sean consideradas como áreas sensibles.
    - Tableros de distribución eléctrica y centros de cableado.
    - Consola de monitoreo de seguridad y vigilancia.
7. Debido a que los Centros de Cómputo de SODIG se definen como áreas restringidas, deben contar con los siguientes mecanismos de protección física, ambiental y controles de acceso:
    - ❖ Acceso mediante mecanismo biométrico y/o tarjeta de aproximación y/o algún otro mecanismo de seguridad.
    - ❖ Detección y extinción de incendios.
    - ❖ Control de humedad y temperatura.
    - ❖ Controles ambientales para aire acondicionado.
    - ❖ Alarmas y cámaras conectadas al circuito cerrado de televisión.
    - ❖ Piso y techo falso.
    - ❖ Energía regulada y sistema de UPS.
8. Las actividades de limpieza en áreas restringidas deben realizarse en horarios en que se encuentre el personal de la unidad correspondiente. Estas actividades serán controladas y supervisadas en todo momento.
9. Se debe contar con planos actualizados de las instalaciones de SODIG, en donde se especifique el nivel de seguridad de cada área, así como la definición del perímetro de seguridad en forma clara. Definir una señalética para la identificación y acceso a estas áreas.
10. Anualmente la Unidad de Gestión de Seguridad de la Información gestionará la ejecución de un estudio de seguridad en las instalaciones físicas de los Centros de Computo a nivel nacional conforme a la planificación establecida, que considere el cumplimiento de la normativas vigentes de los entes reguladores en el ámbito de la seguridad informática; con el objetivo de evaluar los controles de seguridad física implementados, el mismo que debe ser efectuado por personal interno o externo, cuya competencia en seguridad física pueda ser constatada tanto por su experiencia como preparación académica. Dicho estudio debe contar con la cooperación de todas las Unidades de Gestión que se encuentren involucradas y debe contemplar asesoramiento especializado de ser necesario, por ejemplo, temas como: evitar daños causados por fuego, inundación, terremoto, explosión, revueltas sociales y otras formas de desastres naturales o provocados por el hombre. Se debe presentar el resultado del estudio a la Gerencia General, contemplando los planes de acción, fechas y responsables.
11. El personal de guardias de seguridad que presten sus servicios en SODIG debe revisar y verificar que los equipos de computación que salgan de SODIG, tengan su respectiva autorización o a su vez se encuentre registrado su ingreso. Cualquier novedad presentada debe ser comunicada de manera inmediata a la Unidad de Gestión Administrativa Financiera.

12. El cableado de energía eléctrica y de telecomunicaciones, que llevan voz y datos y que dan soporte a los servicios de información, y que se conectan con las instalaciones de procesamiento de información debe protegerse contra cualquier intento de intercepción o daño, contar con instalaciones subterráneas, siempre que sea posible, o sujetas a una adecuada protección alternativa, utilizando conductos seguros.
13. El cableado de energía eléctrica debe estar separado del cableado de comunicaciones y correctamente etiquetado para su fácil identificación. Las unidades de tecnología de cada dependencia deben contar con los planos del cableado eléctrico y de datos, así como también deben tener un control a través de un inventario de puntos de red contrastado con el nombre, ubicación física de cada usuario correspondiente.
14. Las áreas restringidas deben permanecer protegidas por un sistema de alarmas centralizado (control de movimiento y detección de incendio), el cual debe ser monitoreado permanentemente.

4.2.4. LINEAMIENTO DE SEGURIDAD RELACIONADA AL TALENTO HUMANO

a. La Unidad de Gestión de Talento Humano establecerá el procedimiento de selección del personal tomando en consideración la reglamentación vigente, así como también la verificación de los antecedentes penales y la información entregada en la hoja de vida de candidatos, a fin de poder identificar y evitar potenciales riesgos de seguridad de la información.
b. La Unidad de Gestión de Talento Humano informará de manera formal las funciones y responsabilidades que desempeñará para el cumplimiento de sus funciones en SODIG, al momento de la suscripción del contrato.
c. El personal que sea contratado por SODIG bajo cualquiera de las modalidades de contrato deben leer y suscribir una aceptación del Código de Ética de SODIG, así como también un Acuerdo de Confidencialidad vigente, siendo entregados a la Unidad de Gestión de Talento Humano como documento habilitante para proceder con la firma del contrato de vinculación a SODIG. Dichos documentos deben ser anexados al expediente del personal y resguardados en los archivos de Gestión de Talento Humano de SODIG.
d. La Unidad de Gestión de Talento Humano deben gestionar los accesos de usuario de red, correo electrónico y Gestión documental para el personal que se hayan vinculado a SODIG.
e. La dependencia en la que vaya a prestar servicios el personal debe realizar una inducción sobre el correcto manejo de la información de SODIG y el uso de las herramientas informáticas relacionadas con las actividades a desempeñar.
f. La Unidad de Gestión de Seguridad de la Información debe realizar de forma periódica capacitaciones relacionadas con seguridad, responsabilidades legales y los controles de SODIG, así como en el uso correcto de los servicios de información.

4.2.5. LINEAMIENTOS DE RELACIÓN CON PROVEEDORES

I. Únicamente se permitirá el acceso a la información que se encuentre relacionada con el objeto del contrato entre SODIG y el proveedor para prestación de servicios.
II. La Unidad de Gestión responsable del contrato será el responsable también de:
    a. Asegurar que el personal del proveedor que tenga acceso a la información (física y/o digital) administrada por SODIG firme los vigentes.
    b. Garantizar que los recursos que SODIG ponga a disposición del proveedor, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, etc.), serán destinados exclusivamente para cumplir con las obligaciones y propósito del servicio contratado. SODIG

implementará mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

c. Mantener una lista actualizada del personal asignado al servicio, así como también los equipos utilizados en el caso de que el proveedor se conecte a la infraestructura tecnológica de SODIG.

III. Todo proveedor de SODIG que tenga acceso a la información (física y/o digital) administrada por SODIG, debe:

a. Garantizar que su personal cuente con formación y capacitación apropiada para el desarrollo del servicio contratado, tanto a nivel específico en las materias correspondientes a la actividad asociada, así como también en materia de seguridad de la información.
b. Estar obligado durante la vigencia del contrato y después de ello, en mantener la reserva de la información a la que tenga acceso y tendrá prohibido compartirla con terceros o utilizarla para su beneficio.
c. Contar con la autorización de la Unidad Propietaria de la Información a la que preste sus servicios, para poder sacar de las instalaciones de SODIG cualquier activo de la información que sea de propiedad de SODIG.
d. Garantizar el cumplimiento de las restricciones legales respecto del uso del material protegido por normas de propiedad intelectual.
e. Contar con la autorización de la Unidad de Gestión de Seguridad de la Información, para acceder de forma remota a cualquier equipo informático que se encuentre dentro de la infraestructura tecnológica de SODIG.
f. Para conectar sus equipos dentro de la infraestructura tecnológica de SODIG, debe contar con la autorización escrita por parte de la Unidad de Gestión responsable del contrato.
g. Garantizar que el personal asignado para el servicio cumpla con las políticas y lineamientos de seguridad de la información de SODIG.

5. APLICACIÓN DE LA POLÍTICA

Desde la aprobación de este documento, los usuarios internos y externos de SODIG serán responsables de aplicar la política de forma obligatoria en la infraestructura tecnológica de SODIG.

Si para el cumplimiento o apalancamiento del presente documento se requiere de la adquisición de herramientas tecnológicas su aplicación estará sujeto a la compra de la misma.

6. INCUMPLIMIENTO

El incumplimiento de la presente política dará lugar a la aplicación de las sanciones establecidas en el Código del Trabajo, su Reglamento General, así como también las contempladas por la norma interna que se defina para la gestión del talento humano de SODIG.

En el caso que SODIG no se encuentre listo para dar cumplimiento a cualquier punto de la presente política, la unidad responsable de su ejecución debe presentar un informe técnico sustentando las razones por las cuales no se puede dar cumplimiento, conjuntamente de un plan de acción con el respectivo cronograma de trabajo.

En la infraestructura tecnológica existente de SODIG se deberá aplicar de manera progresiva y se considerarán excepciones para ésta implementación, aquellas plataformas tecnológicas que no soporten los lineamientos establecidos; para lo cual, los responsables de su implementación, deberán presentar o avalar técnicamente el informe de justificación y/o un plan de acción para la remediación de la problemática, a la Unidad de Gestión de Seguridad de la Información de SODIG.

7. VIGENCIA Y REVISIÓN

La Política de Seguridad de la Información entrará en vigor inmediatamente después que el mismo haya sido aprobado por las instancias correspondientes.

Para garantizar la efectividad de la presente política, debe ser revisado por lo menos una vez al año o cuando se hubieren producido cambios significativos que impacten estas directrices.

La Unidad de Gestión de Seguridad de la Información es la responsable del manejo de las versiones, así como de las copias controladas del mismo.