|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ENTENDIMIENTO DE TI** | Estructura Organizativa | | **PREGUNTAS** | | | | **OBSERVACIONES** |
| ¿Cómo es la estructura organizativa del departamento de tecnología? | | | |  |
| ¿Cuántas personas aproximadamente estuvieron en el departamento de TI durante el período auditado? | | | |  |
| ¿A quién le reporta la Coordinación de Tecnología? | | | |  |
| ¿Cuáles son las principales responsabilidades del área de tecnología? | | | |  |
| Aplicaciones | | ¿Cuáles son los sistemas o aplicaciones principales que soportan los estados financieros de la Compañía? | | | |  |
| ¿Qué tipo de conexiones o enlaces de comunicación utilizan para conectarse de manera externa e interna en la Compañía? ¿Qué proveedores brindan los servicios de comunicación? | | | |  |
| ¿Se cuenta con un área o proceso que gestione los riesgos de Tecnología de Información? | | | |  |
| Sistema Operativo | | ¿Se tiene un servidor de dominio de manera centralizada para conectarse a la red? ¿Qué sistema Operativo utiliza el servidor de Dominio? | | | |  |
| ¿Cuentan con mecánicos para restringir el acceso a Internet a los usuarios? ¿Por ejemplo un Firewall? | | | |  |
| Base de Datos | | ¿Cuáles son las bases de datos que soportan los sistemas de la Compañía? | | | |  |
| ¿Se tiene documentado e implementado un plan de recuperación en caso de desastres? | | | |  |
| **CONTROLES GENERALES DE TI** |  | Políticas de Seguridad de Información | | **PREGUNTAS** | **Si** | **No** | **OBSERVACIONES** |
| **ACCESOS A PROGRAMAS Y DATOS** | ¿Se cuenta con políticas de seguridad de información formalmente documentada, aprobada y vigente? |  |  |  |
| ¿Se realizan actividades de concientización divulgación de las políticas de seguridad de información al personal de la Compañía? |  |  |  |
| ¿Qué medios son utilizados para divulgar la información, por ejemplo: correos, intranet, firmas de aceptación de las políticas, ¿etc.? |  |  |  |
| ¿Cuáles son las principales responsabilidades del área de tecnología? |  |  |  |
| Acceso físico al hardware del sistema | | ¿Se cuenta con una sala de servidores donde residen los sistemas de la Compañía? |  |  |  |
| ¿Qué mecanismos de restricción de accesos existen para el ingreso a la sala, por ejemplo: lector de tarjetas, huella dactilar, ¿etc.? |  |  |  |
| ¿Quiénes son las personas autorizadas para ingresar a la sala de servidores? |  |  |  |
| Creación y eliminación de cuentas de usuarios | | ¿Existe un proceso de solicitud y aprobación para la creación de usuarios en la red de datos y en los sistemas? |  |  |  |
| ¿Quiénes son las personas autorizadas para la aprobación? ¿Qué mecanismos se utilizan para comunicar y registrar la solicitud? |  |  |  |
| ¿Cómo es el proceso de notificación y eliminación/bloqueo de cuentas de usuarios en la red de datos y en los sistemas? |  |  |  |
| Identificación y autenticación | | ¿Se tienen establecido la utilización de contraseñas para ingresar a la red y a los sistemas? |  |  |  |
|  | ¿Cómo se identifican las cuentas de usuarios en la red y en los sistemas, por ejemplo: inicial del nombre más el apellido? |  |  |  |
| ¿Las contraseñas contemplan aspectos de seguridad tales como: caducidad, longitud mínima, ¿historial de la contraseña y complejidad? |  |  |  |
|  | Monitoreo de accesos en los sistemas | | ¿Se tienen establecidos procedimientos formales para la revisión de la vigencia de los permisos de acceso en los sistemas, que incluya la aprobación formal por parte de los líderes de las distintas áreas? |  |  |  |
| Usuarios con permisos amplios | | ¿Existen usuarios administradores en la red de datos? ¿Quién es el personal autorizado para realizar actividades de administrador en la red de datos? |  |  |  |
|  | ¿Existen usuarios administradores en los sistemas? ¿Quién es el personal autorizado para realizar actividades de administrador en los sistemas? |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ENTENDIMIENTO DE TI** |  | Solicitud, pruebas y aprobaciones de cambios en los sistemas | **PREGUNTAS** | **Si** | **No** | **OBSERVACIONES** |
| **CAMBIOS A PROGRAMAS** | ¿Las solicitudes de cambios son aprobadas? |  |  |  |
| ¿Quién o qué cargos son los responsables de las aprobaciones de las solicitudes? |  |  |  |
| ¿Qué mecanismos de comunicación y registros se utilizan para las aprobaciones de las solicitudes? |  |  |  |
| ¿Se realizan pruebas de los cambios en un ambiente de prueba? |  |  |  |
| ¿Quién o qué cargos son los responsables de realizar las pruebas? |  |  |  |
| ¿Cómo es el proceso de notificación de ejecución de las pruebas? |  |  |  |
| ¿Los pases a producción de los cambios son aprobados? ¿Quién o qué cargos son los responsables de las aprobaciones de los pases a producción? |  |  |  |
| ¿Qué mecanismos de comunicación y registros se utilizan para las aprobaciones de los pases a producción? |  |  |  |
| Ambientes separados en el sistema | ¿Existen servidores o ambientes separados de desarrollo, pruebas y producción en los sistemas? |  |  |  |