| | | |
|---|---|---|
| El campo es de todos Minagricultura | **FORMATO** | VERSIÓN 12 |
| | **MAPA DE RIESGOS** | **F01-PR-SIG-05** |
| | | FECHA EDICIÓN 28/04/2021 |

PROCESO: **Gestión y Gobierno de tecnologías de la Información – TI**

**SECCION B: RIESGOS DE SEGURIDAD DE LA INFORMACION**

| **Identificación del riesgo** | | | | | | **Análisis del riesgo inherente** | | | | | | | | | **Evaluación del nivel de riesgos y definición de controles** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | **EVALUACION DE LA CRITICIDAD DEL ACTIVO** | | | | | | | | **NIVEL DE RIESGO INHERENTE** | | | | | **NIVEL DE RIESGO RESIDUAL** | | | | | | | |
| **ACTIVOS DE INFORMACION** | **TIPO DE ACTIVO** | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | **RIESGO** | **AMENAZA** | **VALORACION DE LA AMENAZA** | **VULNERABILIDAD** | **VALORACION DE VULNERABILIDAD** | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | | | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | **OPCION DE TRATAMIENTO** | **CONTROL** | **Soporte** | **Responsable** |
| | | | | | | | | Acceso remoto no seguro | 2 | | | | | | | | | | 9.1.2 Acceso a redes y servicios de red | | |
| | | | | | | | | Conexiones a red pública desprotegidas | 2 | | | | | | | | | | 13.1.1 Controles de red | | |
| | | | | | | | | | | | | | | | | | | | 13.1.2 Seguridad de servicios de red | | |
| | | | | | | | | | | | | | | | | | | | 13.1.3 Segregación de redes | | |
| | | | | | | | | Eliminación o reutilización de soportes sin borrar | 3 | | | | | | | | | | 8.3.1 Gestión de medios removibles | | |
| | | | | | | | | | | | | | | | | | | | 8.3.2 Desecho de medios | | |
| | | | | | | | | Gestión del control de acceso ineficiente | 2 | | | | | | | | | | 9.4.1 Restricción del acceso a la información | | |
| | | | | | | | | No existen mecanismos de autenticación y validación del usuario | 2 | | | | | | | | | | 9.2.1 Alta y baja de usuario | | |
| | | | | | | | | | | | | | | | | | | | 9.4.2 Procesos de inicio seguro de sesión | | |
| | | | | | | | | | | | | | | | | | | | 9.4.3 Sistema de gestión de contraseña | | |
| | | | | | | | | | | | | | | | | | | | 9.4.4 Uso de programas privilegiados de utilidad | | |
| | | | | | | | | No existen procedimientos formales de revisión de accesos | 2 | | | | | | | | | | 9.2.5 Revisión de los derechos de acceso de usuarios | | |
| | | | | | | | | | | | | | | | | | | | 6.2.2 Teletrabajo | | |
| | | | | | | Acceso no autorizado | 1 | | | | | | | | | | | | 9.1.1 Política de control de acceso | | |
| | | | | | | | | | | | | | | | | | | | 9.2.1 Alta y baja de usuario | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | | | | | NIVEL DE RIESGO INHERENTE | | | | NIVEL DE RIESGO RESIDUAL | | | | | | | |
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| | | | | | | | | No existen procedimientos formales para alta y baja de usuarios | 2 | | | | | | | | 9.2.2 Provisión de acceso a usuarios | | |
| | | | | | | | | | | | | | | | | | 9.2.3 Gestión de derechos de acceso privilegiado | | |
| | | | | | | | | | | | | | | | | | 9.2.4 Gestión de información secreta de autenticación | | |
| | | | | | | | | | | | | | | | | | 9.3.1 Uso de información secreta de autenticación | | |
| | | | | | | | | | | | | | | | | | 9.4.3 Sistema de gestión de contraseña | | |
| | | | | | | | | Uso soportes removibles no controlado | 3 | | | | | | | | 8.1.1 Inventario de activos | | |
| | | | | | | | | | | | | | | | | | 8.1.2 Propiedad de los activos | | |
| | | | | | | | | | | | | | | | | | 8.1.3 Uso aceptable de los activos | | |
| | | | | | | | | | | | | | | | | | 8.3.1 Gestión de medios removibles | | |
| | | | | | | | | | | | | | | | | | 8.3.2 Desecho de medios | | |
| | | | | | | | | | | | | | | | | | 8.3.3 Tránsito de medios físicos | | |
| | | | | | | Escuchas no autorizadas | 1 | Cableado desprotegido | 3 | | | | | | | | 11.2.3 Seguridad del cableado | | |
| | | | | | | | | Comunicaciones a través de redes públicas o desprotegidas | 2 | | | | | | | | 13.1.1 Controles de red | | |
| | | | | | | | | | | | | | | | | | 13.1.2 Seguridad de servicios de red | | |
| | | | | | | | | | | | | | | | | | 13.1.3 Segregación de redes | | |
| | | | | | | | | No existe protección contra código malicioso | 2 | | | | | | | | 12.2.1 Controles contra código malicioso | | |
| | | | | | | | | No existen procedimientos de monitorización de las instalaciones | 3 | | | | | | | | 11.1.2 Controles de acceso físico | | |
| | | | | | | | | | | | | | | | | | 11.1.3 Seguridad de oficinas, salas e instalaciones | | |
| | | | | | | | | | | | | | | | | | 11.1.5 Trabajo en áreas seguras | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | | | | | NIVEL DE RIESGO INHERENTE | | | | NIVEL DE RIESGO RESIDUAL | | | | | | |
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| Planes ejecutados por la OTIC | Información | 2 | 4 | 3 | Perdida de integridad del activo | | | | | 12 | 24 | 9 | 8 | 16 | 6 | Aceptar | 11.1.6 Áreas de entrega y carga | De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin. | Jefe Oficina TIC |
| | | | | | | Manipulación de los registros | 2 | No existe control sobre el uso de utilidades de sistema | 3 | | | | | | | | 12.7.1 Controles de la auditoría de sistemas de información | | |
| | | | | | | | | No existen registros de auditoria | 3 | | | | | | | | 12.4.1 Registro de eventos | | |
| | | | | | | | | | | | | | | | | | 12.4.2 Protección de la información del registro de eventos | | |
| | | | | | | | | | | | | | | | | | 12.4.3 Registro de administrador y operador | | |
| | | | | | | | | | | | | | | | | | 12.4.4 Sincronización de reloj | | |
| | | | | | | Pérdida o corrupción de la información | 1 | No existe protección contra código malicioso | 2 | | | | | | | | 12.2.1 Controles contra código malicioso | | |
| | | | | | | | | | | | | | | | | | 12.3.1 Copia de seguridad de la información | | |
| | | | | | | Revelación de contraseñas | 2 | No existe concienciación y formación en seguridad | 3 | | | | | | | | 7.2.2 Concienciación, educación y capacitación de la seguridad de la información | | |
| | | | | | | | | No existen procesos disciplinarios claros para incidentes de seguridad de la información | 3 | | | | | | | | 7.2.3 Proceso disciplinario | | |
| | | | | | | | | Uso no aceptable de activos | 2 | | | | | | | | 8.1.3 Uso aceptable de los activos | | |
| | | | | | | | | Comunicaciones a través de redes públicas o desprotegidas | 3 | | | | | | | | 13.2.1 Políticas y procedimientos para el intercambio de información | | |
| | | | | | | | | | | | | | | | | | 13.2.2 Acuerdos de intercambio de información | | |
| | | | | | | | | | | | | | | | | | 13.2.3 Mensajería electrónica | | |
| | | | | | | | | | | | | | | | | | 14.1.2 Seguridad del servicio de aplicacion en redes públicas | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | | | | | NIVEL DE RIESGO INHERENTE | | | | NIVEL DE RIESGO RESIDUAL | | | | | | | |
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| | | | | | | | | | | | | | | | | | 14.1.3 Protección de transacciones en servicio de aplicación | | |
| | | | | | | Revelación de información | 2 | | | | | | | | | | 12.1.4 Separación de entornos de desarrollo, prueba y operación | | |
| | | | | | | | | No existe control para copia de información | 2 | | | | | | | | 12.3.1 Copia de seguridad de la información | | |
| | | | | | | | | | | | | | | | | | 8.3.1 Gestión de medios removibles | | |
| | | | | | | | | No existen procedimientos de autorización para información pública | 3 | | | | | | | | 14.1.2 Seguridad del servicio de aplicacion en redes públicas | | |
| | | | | | | | | | | | | | | | | | 8.2.1 Clasificación de la información | | |
| | | | | | | | | No existen procedimientos para el etiquetado y manejo de la información | 3 | | | | | | | | 8.2.2 Etiquetado de la información | | |
| | | | | | | | | | | | | | | | | | 8.2.3 Manejo de activos | | |
| | | | | | | Robo de documentación | 1 | | | | | | | | | | 11.1.2 Controles de acceso físico | | |
| | | | | | | | | | | | | | | | | | 11.1.3 Seguridad de oficinas, salas e instalaciones | | |
| | | | | | | | | Control de acceso al edificio y a las salas ineficiente | 3 | | | | | | | | 11.1.5 Trabajo en áreas seguras | | |
| | | | | | | | | | | | | | | | | | 11.1.6 Áreas de entrega y carga | | |
| | | | | | | | | | | | | | | | | | 11.2.1 Ubicación y protección de equipos | | |
| | | | | | | | | No existen procedimientos de monitorización de las instalaciones | 2 | | | | | | | | 11.1.1 Perímetro de seguridad física | | |
| | | | | | | | | | | | | | | | | | 11.2.7 Seguridad en el desecho o reutilización de equipos | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | | | | | NIVEL DE RIESGO INHERENTE | | | | NIVEL DE RIESGO RESIDUAL | | | | | | | |
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| | | | | | | Robo de información | 1 | Eliminación o reutilización de soportes sin borrar | 3 | | | | | | | | 8.1.4 Devolución de los activos | | |
| | | | | | | | | | | | | | | | | | 8.3.2 Desecho de medios | | |
| | | | | | | | | No existe control para copia de información | 3 | | | | | | | | 12.3.1 Copia de seguridad de la información | | |
| | | | | | | | | | | | | | | | | | 12.4.1 Registro de eventos | | |
| | | | | | | | | | | | | | | | | | 6.2.2 Teletrabajo | | |
| | | | | | | | | | | | | | | | | | 8.3.1 Gestión de medios removibles | | |
| | | | | | | | | | | | | | | | | | 8.3.3 Tránsito de medios físicos | | |
| | | | | | | | | Acceso remoto no seguro | 2 | | | | | | | | 9.1.2 Acceso a redes y servicios de red | | |
| | | | | | | | | Conexiones a red pública desprotegidas | 2 | | | | | | | | 13.1.1 Controles de red | | |
| | | | | | | | | | | | | | | | | | 13.1.2 Seguridad de servicios de red | | |
| | | | | | | | | | | | | | | | | | 13.1.3 Segregación de redes | | |
| | | | | | | | | Eliminación o reutilización de soportes sin borrar | 3 | | | | | | | | 8.3.1 Gestión de medios removibles | | |
| | | | | | | | | | | | | | | | | | 8.3.2 Desecho de medios | | |
| | | | | | | | | Gestión del control de acceso ineficiente | 2 | | | | | | | | 9.4.1 Restricción del acceso a la información | | |
| | | | | | | | | No existen mecanismos de autenticación y validación del usuario | 2 | | | | | | | | 9.2.1 Alta y baja de usuario | | |
| | | | | | | | | | | | | | | | | | 9.4.2 Procesos de inicio seguro de sesión | | |
| | | | | | | | | | | | | | | | | | 9.4.3 Sistema de gestión de contraseña | | |
| | | | | | | | | | | | | | | | | | 9.4.4 Uso de programas privilegiados de utilidad | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | | | | | NIVEL DE RIESGO INHERENTE | | | NIVEL DE RIESGO RESIDUAL | | | | | | | |
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| | | | | | | Acceso no autorizado | 1 | No existen procedimientos formales de revisión de accesos | 2 | | | | | | | | 9.2.5 Revisión de los derechos de acceso de usuarios | | |
| | | | | | | | | No existen procedimientos formales para alta y baja de usuarios | 2 | | | | | | | | 6.2.2 Teletrabajo | | |
| | | | | | | | | | | | | | | | | | 9.1.1 Política de control de acceso | | |
| | | | | | | | | | | | | | | | | | 9.2.1 Alta y baja de usuario | | |
| | | | | | | | | | | | | | | | | | 9.2.2 Provisión de acceso a usuarios | | |
| | | | | | | | | | | | | | | | | | 9.2.3 Gestión de derechos de acceso privilegiado | | |
| | | | | | | | | | | | | | | | | | 9.2.4 Gestión de información secreta de autenticación | | |
| | | | | | | | | | | | | | | | | | 9.3.1 Uso de información secreta de autenticación | | |
| | | | | | | | | | | | | | | | | | 9.4.3 Sistema de gestión de contraseña | | |
| | | | | | | | | Uso soportes removibles no controlado | 3 | | | | | | | | 8.1.1 Inventario de activos | | |
| | | | | | | | | | | | | | | | | | 8.1.2 Propiedad de los activos | | |
| | | | | | | | | | | | | | | | | | 8.1.3 Uso aceptable de los activos | | |
| | | | | | | | | | | | | | | | | | 8.3.1 Gestión de medios removibles | | |
| | | | | | | | | | | | | | | | | | 8.3.2 Desecho de medios | | |
| | | | | | | | | | | | | | | | | | 8.3.3 Tránsito de medios físicos | | |
| | | | | | | | | Cableado desprotegido | 3 | | | | | | | | 11.2.3 Seguridad del cableado | | |
| | | | | | | | | Comunicaciones a través de redes públicas o desprotegidas | 2 | | | | | | | | 13.1.1 Controles de red | | |
| | | | | | | | | | | | | | | | | | 13.1.2 Seguridad de servicios de red | | |
| | | | | | | | | | | | | | | | | | 13.1.3 Segregación de redes | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | NIVEL DE RIESGO INHERENTE | | | NIVEL DE RIESGO RESIDUAL | | | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| | | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | | | | | | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | | | | |
| Repositorio de documentos del proceso | Información | 4 | 4 | 4 | Perdida de confidencialidad, integridad y disponibilidad del activo | Escuchas no autorizadas | 1 | No existe protección contra código malicioso | 2 | 24 | 24 | 18 | 16 | 16 | 12 | Aceptar | 12.2.1 Controles contra código malicioso | De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin. | Jefe Oficina TIC |
| | | | | | | | | No existen procedimientos de monitorización de las instalaciones | 3 | | | | | | | | 11.1.2 Controles de acceso físico | | |
| | | | | | | | | | | | | | | | | | 11.1.3 Seguridad de oficinas, salas e instalaciones | | |
| | | | | | | | | | | | | | | | | | 11.1.5 Trabajo en áreas seguras | | |
| | | | | | | | | | | | | | | | | | 11.1.6 Áreas de entrega y carga | | |
| | | | | | | Manipulación de los registros | 2 | No existe control sobre el uso de utilidades de sistema | 3 | | | | | | | | 12.7.1 Controles de la auditoría de sistemas de información | | |
| | | | | | | | | No existen registros de auditoria | 3 | | | | | | | | 12.4.1 Registro de eventos | | |
| | | | | | | | | | | | | | | | | | 12.4.2 Protección de la información del registro de eventos | | |
| | | | | | | | | | | | | | | | | | 12.4.3 Registro de administrador y operador | | |
| | | | | | | | | | | | | | | | | | 12.4.4 Sincronización de reloj | | |
| | | | | | | Pérdida o corrupción de la información | 1 | No existe protección contra código malicioso | 2 | | | | | | | | 12.2.1 Controles contra código malicioso | | |
| | | | | | | | | | | | | | | | | | 12.3.1 Copia de seguridad de la información | | |
| | | | | | | Revelación de contraseñas | 2 | No existe concienciación y formación en seguridad | 3 | | | | | | | | 7.2.2 Concienciación, educación y capacitación de la seguridad de la información | | |
| | | | | | | | | No existen procesos disciplinarios claros para incidentes de seguridad de la información | 3 | | | | | | | | 7.2.3 Proceso disciplinario | | |
| | | | | | | | | Uso no aceptable de activos | 2 | | | | | | | | 8.1.3 Uso aceptable de los activos | | |
| | | | | | | | | | | | | | | | | | 13.2.1 Políticas y procedimientos para el intercambio de información | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | | | | | NIVEL DE RIESGO INHERENTE | | | | NIVEL DE RIESGO RESIDUAL | | | | | | |
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| | | | | | | Revelación de información | 2 | Comunicaciones a través de redes públicas o desprotegidas | 3 | | | | | | | | 13.2.2 Acuerdos de intercambio de información | | |
| | | | | | | | | | | | | | | | | | 13.2.3 Mensajería electrónica | | |
| | | | | | | | | | | | | | | | | | 14.1.2 Seguridad del servicio de aplicacion en redes públicas | | |
| | | | | | | | | | | | | | | | | | 14.1.3 Protección de transacciones en servicio de aplicación | | |
| | | | | | | | | No existe control para copia de información | 2 | | | | | | | | 12.1.4 Separación de entornos de desarrollo, prueba y operación | | |
| | | | | | | | | | | | | | | | | | 12.3.1 Copia de seguridad de la información | | |
| | | | | | | | | | | | | | | | | | 8.3.1 Gestión de medios removibles | | |
| | | | | | | | | No existen procedimientos de autorización para información pública | 3 | | | | | | | | 14.1.2 Seguridad del servicio de aplicacion en redes públicas | | |
| | | | | | | | | No existen procedimientos para el etiquetado y manejo de la información | 3 | | | | | | | | 8.2.1 Clasificación de la información | | |
| | | | | | | | | | | | | | | | | | 8.2.2 Etiquetado de la información | | |
| | | | | | | | | | | | | | | | | | 8.2.3 Manejo de activos | | |
| | | | | | | Robo de documentación | 2 | Control de acceso al edificio y a las salas ineficiente | 3 | | | | | | | | 11.1.2 Controles de acceso físico | | |
| | | | | | | | | | | | | | | | | | 11.1.3 Seguridad de oficinas, salas e instalaciones | | |
| | | | | | | | | | | | | | | | | | 11.1.5 Trabajo en áreas seguras | | |
| | | | | | | | | | | | | | | | | | 11.1.6 Áreas de entrega y carga | | |
| | | | | | | | | | | | | | | | | | 11.2.1 Ubicación y protección de equipos | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | | | | | NIVEL DE RIESGO INHERENTE | | | | NIVEL DE RIESGO RESIDUAL | | | | | | | |
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| | | | | | | | | No existen procedimientos de monitorización de las instalaciones | 2 | | | | | | | | 11.1.1 Perímetro de seguridad física | | |
| | | | | | | Robo de información | 2 | Eliminación o reutilización de soportes sin borrar | 3 | | | | | | | | 11.2.7 Seguridad en el desecho o reutilización de equipos | | |
| | | | | | | | | | | | | | | | | | 8.1.4 Devolución de los activos | | |
| | | | | | | | | | | | | | | | | | 8.3.2 Desecho de medios | | |
| | | | | | | | | No existe control para copia de información | 3 | | | | | | | | 12.3.1 Copia de seguridad de la información | | |
| | | | | | | | | | | | | | | | | | 12.4.1 Registro de eventos | | |
| | | | | | | | | | | | | | | | | | 6.2.2 Teletrabajo | | |
| | | | | | | | | | | | | | | | | | 8.3.1 Gestión de medios removibles | | |
| | | | | | | | | | | | | | | | | | 8.3.3 Tránsito de medios físicos | | |
| | | | | | | | | Acceso remoto no seguro | 2 | | | | | | | | 9.1.2 Acceso a redes y servicios de red | | |
| | | | | | | | | Conexiones a red pública desprotegidas | 2 | | | | | | | | 13.1.1 Controles de red | | |
| | | | | | | | | | | | | | | | | | 13.1.2 Seguridad de servicios de red | | |
| | | | | | | | | | | | | | | | | | 13.1.3 Segregación de redes | | |
| | | | | | | | | Eliminación o reutilización de soportes sin borrar | 3 | | | | | | | | 8.3.1 Gestión de medios removibles | | |
| | | | | | | | | | | | | | | | | | 8.3.2 Desecho de medios | | |
| | | | | | | | | Gestión del control de acceso ineficiente | 2 | | | | | | | | 9.4.1 Restricción del acceso a la información | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | | | | | NIVEL DE RIESGO INHERENTE | | | | NIVEL DE RIESGO RESIDUAL | | | | | | |
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| | | | | | | Acceso no autorizado | 1 | No existen mecanismos de autenticación y validación del usuario | 2 | | | | | | | | 9.2.1 Alta y baja de usuario<br>9.4.2 Procesos de inicio seguro de sesión<br>9.4.3 Sistema de gestión de contraseña<br>9.4.4 Uso de programas privilegiados de utilidad | | |
| | | | | | | | | No existen procedimientos formales de revisión de accesos | 2 | | | | | | | | 9.2.5 Revisión de los derechos de acceso de usuarios<br>6.2.2 Teletrabajo<br>9.1.1 Política de control de acceso | | |
| | | | | | | | | No existen procedimientos formales para alta y baja de usuarios | 2 | | | | | | | | 9.2.1 Alta y baja de usuario<br>9.2.2 Provisión de acceso a usuarios<br>9.2.3 Gestión de derechos de acceso privilegiado<br>9.2.4 Gestión de información secreta de autenticación<br>9.3.1 Uso de información secreta de autenticación<br>9.4.3 Sistema de gestión de contraseña | | |
| | | | | | | | | Uso soportes removibles no | 3 | | | | | | | | 8.1.1 Inventario de activos<br>8.1.2 Propiedad de los activos<br>8.1.3 Uso aceptable de los activos | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | | | | | NIVEL DE RIESGO INHERENTE | | | | NIVEL DE RIESGO RESIDUAL | | | | | | |
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| Reportes e informes de gestión | Información | 2 | 4 | 3 | Perdida de integridad del activo | | | controlado | | 12 | 24 | 9 | 8 | 16 | 6 | Aceptar | 8.3.1 Gestión de medios removibles | De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin. | Jefe Oficina TIC |
| | | | | | | | | | | | | | | | | | 8.3.2 Desecho de medios | | |
| | | | | | | | | | | | | | | | | | 8.3.3 Tránsito de medios físicos | | |
| | | | | | | Escuchas no autorizadas | 1 | Cableado desprotegido | 3 | | | | | | | | 11.2.3 Seguridad del cableado | | |
| | | | | | | | | Comunicaciones a través de redes públicas o desprotegidas | 2 | | | | | | | | 13.1.1 Controles de red | | |
| | | | | | | | | | | | | | | | | | 13.1.2 Seguridad de servicios de red | | |
| | | | | | | | | | | | | | | | | | 13.1.3 Segregación de redes | | |
| | | | | | | | | No existe protección contra código malicioso | 2 | | | | | | | | 12.2.1 Controles contra código malicioso | | |
| | | | | | | | | No existen procedimientos de monitorización de las instalaciones | 3 | | | | | | | | 11.1.2 Controles de acceso físico | | |
| | | | | | | | | | | | | | | | | | 11.1.3 Seguridad de oficinas, salas e instalaciones | | |
| | | | | | | | | | | | | | | | | | 11.1.5 Trabajo en áreas seguras | | |
| | | | | | | | | | | | | | | | | | 11.1.6 Áreas de entrega y carga | | |
| | | | | | | Manipulación de los registros | 2 | No extiste control sobre el uso de utilizadades del sistema | 3 | | | | | | | | 12.7.1 Controles de la auditoría de sistemas de información | | |
| | | | | | | | | No existen registros de auditoria | 3 | | | | | | | | 12.4.1 Registro de eventos | | |
| | | | | | | | | | | | | | | | | | 12.4.2. Protección de la información del registo de eventos | | |
| | | | | | | | | | | | | | | | | | 12.4.3 Resgistro de administrador y operador | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | | | | | NIVEL DE RIESGO INHERENTE | | | | NIVEL DE RIESGO RESIDUAL | | | | | | | |
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| | | | | | | | | | | | | | | | | | 12.4.4 Sincronización de reloj | | |
| | | | | | | Pérdida o corrupción de la información | 1 | No existe protección contra código malicioso | 2 | | | | | | | | 12.2.1. Controles contra codigo malicioso | | |
| | | | | | | | | | | | | | | | | | 12.3.1 Copia de seguridad de la información | | |
| | | | | | | Revelación de contraseñas | 2 | No existe concienciación y formación en seguridad | 3 | | | | | | | | 7.2.2. Concienciación, educación y capacitación de la seguridad de la información | | |
| | | | | | | | | No existen procesos disciplinarios claros para incidentes de seguridad de la información | 3 | | | | | | | | 7.2.3 Proceso disciplinario | | |
| | | | | | | | | Uso no aceptable de activos | 2 | | | | | | | | 8.1.3 Uso aceptable de los activos | | |
| | | | | | | Revelación de información | 2 | Comunicaciones a través de redes públicas o desprotegidas | 3 | | | | | | | | 13.2.1 Políticas y procedimientos para el intercambio de información | | |
| | | | | | | | | | | | | | | | | | 13.2.2 Acuerdos de intercambio de información | | |
| | | | | | | | | | | | | | | | | | 13.2.3 Mensajería electrónica | | |
| | | | | | | | | | | | | | | | | | 14.1.2 Seguridad del servicio de aplicacion en redes públicas | | |
| | | | | | | | | | | | | | | | | | 14.1.3 Protección de transacciones en servicio de aplicación | | |
| | | | | | | | | No existe control para copia de información | 2 | | | | | | | | 12.1.4 Separación de entornos de desarrollo, prueba y operación | | |
| | | | | | | | | | | | | | | | | | 12.3.1 Copia de seguridad de la información | | |
| | | | | | | | | | | | | | | | | | 8.3.1 Gestión de medios removibles | | |
| | | | | | | | | No existe procedimiento de autorización para la información pública | 3 | | | | | | | | 14.1.2 Seguridad de los servicios de aplicación en redes publicas | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | | | | | NIVEL DE RIESGO INHERENTE | | | | NIVEL DE RIESGO RESIDUAL | | | | | | | |
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| | | | | | | | | No existen procedimientos para el etiquetado y manejo de la información | 3 | | | | | | | | 8.2.1 Clasificación de la información | | |
| | | | | | | | | | | | | | | | | | 8.2.2. Etiqetado de la información | | |
| | | | | | | | | | | | | | | | | | 8.2.3 Manejo de activos | | |
| | | | | | | Robo de documentación | 1 | Control de acceso al edificio y a las salas ineficiente | 3 | | | | | | | | 11.1.2 Controles de acceso físico | | |
| | | | | | | | | | | | | | | | | | 11.1.3 Seguridad de oficinas, salas e instalaciones | | |
| | | | | | | | | | | | | | | | | | 11.1.5 Trabajo en areas seguras | | |
| | | | | | | | | | | | | | | | | | 11.1.6 Áreas de entrega y carga | | |
| | | | | | | | | | | | | | | | | | 11.2.1 Ubicación y protección de equipos | | |
| | | | | | | | | No existen procedimientos de monitorización de las instalaciones | 2 | | | | | | | | 11.1.1 Perímetro de seguridad física | | |
| | | | | | | Robo de información | 1 | Eliminación o reutilización de soportes sin borrar | 3 | | | | | | | | 11.2.7 Seguridad en el desecho o reutilización de equipos | | |
| | | | | | | | | | | | | | | | | | 8.1.4 Devolución de los activos | | |
| | | | | | | | | | | | | | | | | | 8.3.2 Desecho de medios | | |
| | | | | | | | | No exite control para copia de la información | 3 | | | | | | | | 12.3.1 Copia de seguridad de la información | | |
| | | | | | | | | | | | | | | | | | 12.4.1 Registo de eventos | | |
| | | | | | | | | | | | | | | | | | 6.2.2 Teletrabajo | | |
| | | | | | | | | | | | | | | | | | 8.3.1 Gestión de medios removibles | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | | | | | | NIVEL DE RIESGO INHERENTE | | | NIVEL DE RIESGO RESIDUAL | | | | | | | |
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| | | | | | | | | | | | | | | | | | 8.3.3 Tránsito de medios físicos | | |
| | | | | | | Acceso no autorizado | 1 | Acceso remoto no seguro | 2 | | | | | | | | 9.1.2 Acceso a redes y servicios de red | | |
| | | | | | | | | Conexiones a red pública desprotegidas | 2 | | | | | | | | 13.1.1 Controles de red<br>13.1.2 Seguridad de servicios de red<br>13.1.3 Segregación de redes | | |
| | | | | | | | | Eliminación o reutilización de soportes sin borrar | 3 | | | | | | | | 8.3.1 Gestión de medios removibles<br>8.3.2 Desecho de medios | | |
| | | | | | | | | Gestión del control de acceso ineficiente | 2 | | | | | | | | 9.4.1 Restricción del acceso a la información | | |
| | | | | | | | | No existen mecanismos de autenticación y validación del usuario | 2 | | | | | | | | 9.2.1 Alta y baja de usuario<br>9.4.2 Procesos de inicio seguro de sesión<br>9.4.3 Sistema de gestión de contraseña<br>9.4.4 Uso de programas privilegiados de utilidad | | |
| | | | | | | | | No existen procedimientos formales de revisión de accesos | 2 | | | | | | | | 9.2.5 Revisión de los derechos de acceso de usuarios | | |
| | | | | | | | | No existen procedimientos formales para alta y baja de usuarios | 2 | | | | | | | | 6.2.2 Teletrabajo<br>9.1.1 Política de control de acceso<br>9.2.1 Alta y baja de usuario<br>9.2.2 Provisión de acceso a usuarios<br>9.2.3 Gestión de derechos de acceso privilegiado<br>9.2.4 Gestión de información secreta de autenticación<br>9.3.1 Uso de información secreta de autenticación<br>9.4.3 Sistema de gestión de contraseña | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | | | | | | NIVEL DE RIESGO INHERENTE | | | NIVEL DE RIESGO RESIDUAL | | | | | | | |
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| Actas de comité de gobierno | Información | 2 | 4 | 2 | Perdida de integridad del activo | Escuchas no autorizadas | 1 | Uso soportes removibles no controlado | 3 | 18 | 24 | 18 | 12 | 16 | 12 | Aceptar | 8.1.1 Inventario de activos | De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin. | Jefe Oficina TIC |
| | | | | | | | | | | | | | | | | | 8.1.2 Propiedad de los activos | | |
| | | | | | | | | | | | | | | | | | 8.1.3 Uso aceptable de los activos | | |
| | | | | | | | | | | | | | | | | | 8.3.1 Gestión de medios removibles | | |
| | | | | | | | | | | | | | | | | | 8.3.2 Desecho de medios | | |
| | | | | | | | | | | | | | | | | | 8.3.3 Tránsito de medios físicos | | |
| | | | | | | | | Cableado desprotegido | 3 | | | | | | | | 11.2.3 Seguridad del cableado | | |
| | | | | | | | | Comunicaciones a través de redes públicas o desprotegidas | 2 | | | | | | | | 13.1.1 Controles de red | | |
| | | | | | | | | | | | | | | | | | 13.1.2 Seguridad de servicios de red | | |
| | | | | | | | | | | | | | | | | | 13.1.3 Segregación de redes | | |
| | | | | | | | | No existe protección contra código malicioso | 2 | | | | | | | | 12.2.1 Controles contra código malicioso | | |
| | | | | | | | | No existen procedimientos de monitorización de las instalaciones | 2 | | | | | | | | 11.1.2 Controles de acceso físico | | |
| | | | | | | | | | | | | | | | | | 11.1.3 Seguridad de oficinas, salas e instalaciones | | |
| | | | | | | | | | | | | | | | | | 11.1.5 Trabajo en áreas seguras | | |
| | | | | | | | | | | | | | | | | | 11.1.6 Áreas de entrega y carga | | |
| | | | | | | Manipulación de los registros | 2 | No existe control sobre el uso de utilidades de sistema | 3 | | | | | | | | 12.7.1 Controles de la auditoría de sistemas de información | | |
| | | | | | | | | No existen registros de auditoria | 3 | | | | | | | | 12.4.1 Registro de eventos | | |
| | | | | | | | | | | | | | | | | | 12.4.2 Protección de la información del registro de eventos | | |
| | | | | | | | | | | | | | | | | | 12.4.3 Registro de administrador y operador | | |
| | | | | | | | | | | | | | | | | | 12.4.4 Sincronización de reloj | | |
| | | | | | | Pérdida o corrupción de la información | 1 | No existe protección contra | 2 | | | | | | | | 12.2.1 Controles contra código malicioso | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | | | | | NIVEL DE RIESGO INHERENTE | | | | NIVEL DE RIESGO RESIDUAL | | | | | | |
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| | | | | | | Pérdida o corrupción de la información | 1 | código malicioso | 2 | | | | | | | | 12.3.1 Copia de seguridad de la información | | |
| | | | | | | Revelación de contraseñas | 2 | No existe concienciación y formación en seguridad | 3 | | | | | | | | 7.2.2 Concienciación, educación y capacitación de la seguridad de la información | | |
| | | | | | | | | No existen procesos disciplinarios claros para incidentes de seguridad de la | 3 | | | | | | | | 7.2.3 Proceso disciplinario | | |
| | | | | | | | | Uso no aceptable de activos | 2 | | | | | | | | 8.1.3 Uso aceptable de los activos | | |
| | | | | | | Revelación de información | 2 | Comunicaciones a través de redes públicas o desprotegidas | 3 | | | | | | | | 13.2.1 Políticas y procedimientos para el intercambio de información | | |
| | | | | | | | | | | | | | | | | | 13.2.2 Acuerdos de intercambio de información | | |
| | | | | | | | | | | | | | | | | | 13.2.3 Mensajería electrónica | | |
| | | | | | | | | | | | | | | | | | 14.1.2 Seguridad del servicio de aplicacion en redes públicas | | |
| | | | | | | | | | | | | | | | | | 14.1.3 Protección de transacciones en servicio de aplicación | | |
| | | | | | | | | No existe control para copia de información | 2 | | | | | | | | 12.1.4 Separación de entornos de desarrollo, prueba y operación | | |
| | | | | | | | | | | | | | | | | | 12.3.1 Copia de seguridad de la información | | |
| | | | | | | | | | | | | | | | | | 8.3.1 Gestión de medios removibles | | |
| | | | | | | | | No existen procedimientos de autorización para información pública | 3 | | | | | | | | 14.1.2 Seguridad del servicio de aplicacion en redes públicas | | |
| | | | | | | | | No existen procedimientos para el etiquetado y manejo de la información | 3 | | | | | | | | 8.2.1 Clasificación de la información | | |
| | | | | | | | | | | | | | | | | | 8.2.2 Etiquetado de la información | | |
| | | | | | | | | | | | | | | | | | 8.2.3 Manejo de activos | | |
| | | | | | | Robo de documentación | 3 | Control de acceso al edificio y a las salas ineficiente | 3 | | | | | | | | 11.1.2 Controles de acceso físico | | |
| | | | | | | | | | | | | | | | | | 11.1.3 Seguridad de oficinas, salas e instalaciones | | |
| | | | | | | | | | | | | | | | | | 11.1.5 Trabajo en áreas seguras | | |
| | | | | | | | | | | | | | | | | | 11.1.6 Áreas de entrega y carga | | |
| | | | | | | | | | | | | | | | | | 11.2.1 Ubicación y protección de equipos | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | | | | | NIVEL DE RIESGO INHERENTE | | | NIVEL DE RIESGO RESIDUAL | | | | | | | | |
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| | | | | | | | | No existen procedimientos de monitorización de las instalaciones | 2 | | | | | | | | 11.1.1 Perímetro de seguridad física | | |
| | | | | | | Robo de información | 2 | Eliminación o reutilización de soportes sin borrar | 3 | | | | | | | | 11.2.7 Seguridad en el desecho o reutilización de equipos | | |
| | | | | | | | | | | | | | | | | | 8.1.4 Devolución de los activos | | |
| | | | | | | | | | | | | | | | | | 8.3.2 Desecho de medios | | |
| | | | | | | | | No existe control para copia de información | 3 | | | | | | | | 12.3.1 Copia de seguridad de la información | | |
| | | | | | | | | | | | | | | | | | 12.4.1 Registro de eventos | | |
| | | | | | | | | | | | | | | | | | 6.2.2 Teletrabajo | | |
| | | | | | | | | | | | | | | | | | 8.3.1 Gestión de medios removibles | | |
| | | | | | | | | | | | | | | | | | 8.3.3 Tránsito de medios físicos | | |
| | | | | | | | | Acceso remoto no seguro | 2 | | | | | | | | 9.1.2 Acceso a redes y servicios de red | | |
| | | | | | | | | Conexiones a red pública desprotegidas | 2 | | | | | | | | 13.1.1 Controles de red | | |
| | | | | | | | | | | | | | | | | | 13.1.2 Seguridad de servicios de red | | |
| | | | | | | | | | | | | | | | | | 13.1.3 Segregación de redes | | |
| | | | | | | | | Eliminación o reutilización de soportes sin borrar | 3 | | | | | | | | 8.3.1 Gestión de medios removibles | | |
| | | | | | | | | | | | | | | | | | 8.3.2 Desecho de medios | | |
| | | | | | | | | Gestión del control de acceso ineficiente | 2 | | | | | | | | 9.4.1 Restricción del acceso a la información | | |
| | | | | | | | | No existen mecanismos de autenticación y validación del usuario | 2 | | | | | | | | 9.2.1 Alta y baja de usuario | | |
| | | | | | | | | | | | | | | | | | 9.4.2 Procesos de inicio seguro de sesión | | |
| | | | | | | | | | | | | | | | | | 9.4.3 Sistema de gestión de contraseña | | |
| | | | | | | | | | | | | | | | | | 9.4.4 Uso de programas privilegiados de utilidad | | |
| | | | | | | | | No existen procedimientos formales de revisión de accesos | 2 | | | | | | | | 9.2.5 Revisión de los derechos de acceso de usuarios | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | | | | | NIVEL DE RIESGO INHERENTE | | | | NIVEL DE RIESGO RESIDUAL | | | | | | | |
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| | | | | | | Acceso no autorizado | 1 | No existen procedimientos formales para alta y baja de usuarios | 2 | | | | | | | | 6.2.2 Teletrabajo | | |
| | | | | | | | | | | | | | | | | | 9.1.1 Política de control de acceso | | |
| | | | | | | | | | | | | | | | | | 9.2.1 Alta y baja de usuario | | |
| | | | | | | | | | | | | | | | | | 9.2.2 Provisión de acceso a usuarios | | |
| | | | | | | | | | | | | | | | | | 9.2.3 Gestión de derechos de acceso privilegiado | | |
| | | | | | | | | | | | | | | | | | 9.2.4 Gestión de información secreta de autenticación | | |
| | | | | | | | | | | | | | | | | | 9.3.1 Uso de información secreta de autenticación | | |
| | | | | | | | | | | | | | | | | | 9.4.3 Sistema de gestión de contraseña | | |
| | | | | | | | | Uso soportes removibles no controlado | 3 | | | | | | | | 8.1.1 Inventario de activos | | |
| | | | | | | | | | | | | | | | | | 8.1.2 Propiedad de los activos | | |
| | | | | | | | | | | | | | | | | | 8.1.3 Uso aceptable de los activos | | |
| | | | | | | | | | | | | | | | | | 8.3.1 Gestión de medios removibles | | |
| | | | | | | | | | | | | | | | | | 8.3.2 Desecho de medios | | |
| | | | | | | | | | | | | | | | | | 8.3.3 Tránsito de medios físicos | | |
| | | | | | | Escuchas no autorizadas | 1 | Cableado desprotegido | 3 | | | | | | | | 11.2.3 Seguridad del cableado | | |
| | | | | | | | | Comunicaciones a través de redes públicas o desprotegidas | 2 | | | | | | | | 13.1.1 Controles de red | | |
| | | | | | | | | | | | | | | | | | 13.1.2 Seguridad de servicios de red | | |
| | | | | | | | | | | | | | | | | | 13.1.3 Segregación de redes | | |
| | | | | | | | | No existe protección contra código malicioso | 2 | | | | | | | | 12.2.1 Controles contra código malicioso | | |
| | | | | | | | | No existen procedimientos de monitorización de las | 3 | | | | | | | | 11.1.2 Controles de acceso físico | | |
| | | | | | | | | | | | | | | | | | 11.1.3 Seguridad de oficinas, salas e instalaciones | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | | | | | NIVEL DE RIESGO INHERENTE | | | | NIVEL DE RIESGO RESIDUAL | | | | | | | |
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| Reportes de transformación digital sectorial | Información | 2 | 4 | 3 | Perdida de integridad del activo | | | Monitorización de las instalaciones | 3 | 12 | 24 | 9 | 8 | 16 | 6 | Aceptar | 11.1.5 Trabajo en áreas seguras | De conformidad con la Política de Seguridad y Privacidad de la Información, la gestión del Sistema de Gestión de Seguridad de la Información, la documentación de la implementación de controles se realiza directamente en la plataforma dispuesta para tal fin. | Jefe Oficina TIC |
| | | | | | | | | | | | | | | | | | 11.1.6 Áreas de entrega y carga | | |
| | | | | | | Manipulación de los registros | 2 | No existe control sobre el uso de utilidades de sistema | 3 | | | | | | | | 12.7.1 Controles de la auditoría de sistemas de información | | |
| | | | | | | | | No existen registros de auditoria | 3 | | | | | | | | 12.4.1 Registro de eventos | | |
| | | | | | | | | | | | | | | | | | 12.4.2 Protección de la información del registro de eventos | | |
| | | | | | | | | | | | | | | | | | 12.4.3 Registro de administrador y operador | | |
| | | | | | | | | | | | | | | | | | 12.4.4 Sincronización de reloj | | |
| | | | | | | Pérdida o corrupción de la información | 1 | No existe protección contra código malicioso | 2 | | | | | | | | 12.2.1 Controles contra código malicioso | | |
| | | | | | | | | | | | | | | | | | 12.3.1 Copia de seguridad de la información | | |
| | | | | | | Revelación de contraseñas | 2 | No existe concienciación y formación en seguridad | 3 | | | | | | | | 7.2.2 Concienciación, educación y capacitación de la seguridad de la información | | |
| | | | | | | | | No existen procesos disciplinarios claros para incidentes de seguridad de la | 3 | | | | | | | | 7.2.3 Proceso disciplinario | | |
| | | | | | | | | Uso no aceptable de activos | 2 | | | | | | | | 8.1.3 Uso aceptable de los activos | | |
| | | | | | | Revelación de información | 2 | Comunicaciones a través de redes públicas o desprotegidas | 3 | | | | | | | | 13.2.1 Políticas y procedimientos para el intercambio de información | | |
| | | | | | | | | | | | | | | | | | 13.2.2 Acuerdos de intercambio de información | | |
| | | | | | | | | | | | | | | | | | 13.2.3 Mensajería electrónica | | |
| | | | | | | | | | | | | | | | | | 14.1.2 Seguridad del servicio de aplicacion en redes públicas | | |
| | | | | | | | | | | | | | | | | | 14.1.3 Protección de transacciones en servicio de aplicación | | |
| | | | | | | | | No existe control para copia de información | 2 | | | | | | | | 12.1.4 Separación de entornos de desarrollo, prueba y operación | | |
| | | | | | | | | | | | | | | | | | 12.3.1 Copia de seguridad de la información | | |
| | | | | | | | | | | | | | | | | | 8.3.1 Gestión de medios removibles | | |
| | | | | | | | | No existen procedimientos de autorización para información pública | 3 | | | | | | | | 14.1.2 Seguridad del servicio de aplicacion en redes públicas | | |

| Identificación del riesgo | | | | | | Análisis del riesgo inherente | | | | | | | Evaluación del nivel de riesgos y definición de controles | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | EVALUACION DE LA CRITICIDAD DEL ACTIVO | | | | | | | NIVEL DE RIESGO INHERENTE | | | | NIVEL DE RIESGO RESIDUAL | | | | | | | |
| ACTIVOS DE INFORMACION | TIPO DE ACTIVO | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | RIESGO | AMENAZA | VALORACION DE LA AMENAZA | VULNERABILIDAD | VALORACION DE VULNERABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | CONFIDENCIALIDAD | INTEGRIDAD | DISPONSABILIDAD | OPCION DE TRATAMIENTO | CONTROL | Soporte | Responsable |
| | | | | | | | | No existen procedimientos para el etiquetado y manejo de la información | 3 | | | | | | | | 8.2.1 Clasificación de la información | | |
| | | | | | | | | | | | | | | | | | 8.2.2 Etiquetado de la información | | |
| | | | | | | | | | | | | | | | | | 8.2.3 Manejo de activos | | |
| | | | | | | Robo de documentación | 1 | Control de acceso al edificio y a las salas ineficiente | 3 | | | | | | | | 11.1.2 Controles de acceso físico | | |
| | | | | | | | | | | | | | | | | | 11.1.3 Seguridad de oficinas, salas e instalaciones | | |
| | | | | | | | | | | | | | | | | | 11.1.5 Trabajo en áreas seguras | | |
| | | | | | | | | | | | | | | | | | 11.1.6 Áreas de entrega y carga | | |
| | | | | | | | | | | | | | | | | | 11.2.1 Ubicación y protección de equipos | | |
| | | | | | | | | No existen procedimientos de monitorización de las instalaciones | 2 | | | | | | | | 11.1.1 Perímetro de seguridad física | | |
| | | | | | | Robo de información | 1 | Eliminación o reutilización de soportes sin borrar | 3 | | | | | | | | 11.2.7 Seguridad en el desecho o reutilización de equipos | | |
| | | | | | | | | | | | | | | | | | 8.1.4 Devolución de los activos | | |
| | | | | | | | | | | | | | | | | | 8.3.2 Desecho de medios | | |
| | | | | | | | | No existe control para copia de información | 3 | | | | | | | | 12.3.1 Copia de seguridad de la información | | |
| | | | | | | | | | | | | | | | | | 12.4.1 Registro de eventos | | |
| | | | | | | | | | | | | | | | | | 6.2.2 Teletrabajo | | |
| | | | | | | | | | | | | | | | | | 8.3.1 Gestión de medios removibles | | |
| | | | | | | | | | | | | | | | | | 8.3.3 Tránsito de medios físicos | | |

| | REVISO | APROBO |
|---|---|---|
| Firma | | |
| Nombre | **José Vicente Franco Martínez** | **Alfonso Javier Celedón Simón** |
| Cargo | Profesional Especializado Oficina TIC | Jefe Oficina de Tecnologías de la Información y las Comunicaciones |
| Fecha | 03 de julio de 2021 | 03 de julio de 2021 |