**Control de versionamiento del Documento**

| Versión | Elaborado por: | Cambios: |
|---|---|---|
| 1 | Rony González Sánchez<br>José Humberto Colo<br>**Cargo:** Consultores Seguridad de la Información<br>**Fecha:** septiembre de 2019 | Creación del documento con el detalle del diagnóstico realizado y los resultados según criterios de evaluación. |

# Contenido

# 1. Diagnóstico Situación Actual Empresa Educativa (Capacitadora):

Con la revisión realizada a la empresa sobre cada control, concluimos que la empresa se encuentra en un nivel de madurez en seguridad igual a Nivel 0: No existente, requiere definir, documentar, implementar, formalizar y divulgar la gran mayoría de controles de seguridad bajo los controles propuestos por la norma en referencia, se identificó que la empresa cuenta con algunos fundamentos en la definición de la seguridad de la información, por ejemplo en los controles de seguridad definidos en el dominio de recursos humanos, existe un mayor nivel de madurez en cuanto a seguridad; así como la existencia de lineamientos de seguridad los cuales deben ser apoyados por la alta dirección, con base en los resultados de este diagnóstico, la empresa nota con preocupación la situación y con apoyo de los altos directivos mostrará este ejercicio y buscará aumentar los recursos en donde sean aplicables para comprender y mejorar en los aspectos de seguridad.

A partir del contexto de los diferentes dominios y controles propuestos por la norma ISO/IEC 27001:2013, se evaluó la dimensión de operatividad (madurez), la cual fue tomada del Framework de COBIT 4.1, cuyo objeto es la administración del proceso de monitorear y evaluar el control interno para satisfacer el requerimiento de negocio de TI de proteger el logro de los objetivos de TI y cumplir con las leyes y regulaciones con TI [1], con los siguientes niveles:

• Nivel 0: No existente

Cuando la organización carece de procedimientos para monitorear la efectividad de los controles internos. Los métodos de reporte de control interno gerenciales no existen. Existe una falta generalizada de conciencia sobre seguridad operativa y el aseguramiento del control interno de la TI. La gerencia y los empleados no tienen conciencia general sobre el control interno.

• Nivel 1: Inicial/Ad Hoc

Cuando la gerencia reconoce la necesidad de administrar y asegurar el control de TI de forma regular. La experiencia individual para evaluar la suficiencia del control interno se aplica de forma ad hoc. La gerencia de TI no ha asignado de manera formal las responsabilidades para monitorear la efectividad de los controles internos. Las evaluaciones de control interno de TI se realizan como parte de las auditorías financieras tradicionales, con metodologías y habilidades que no reflejan las necesidades de la función de los servicios de información.

• Nivel 2: Repetible pero intuitivo

Cuando la organización utiliza reportes de control informales para comenzar iniciativas de acción correctiva. La evaluación de control interno depende de las habilidades de individuos clave. La organización tiene una mayor conciencia sobre el monitoreo de los controles internos. La gerencia de servicios de información realiza monitoreo periódico sobre la efectividad de lo que considera controles internos críticos. Se están empezando a utilizar metodologías y herramientas para monitorear los controles internos, aunque no se basan en un plan. Los factores de riesgo específicos del ambiente de TI se identifican con base en las habilidades de individuos.

• Nivel 3: Definido

Cuando la gerencia apoya y ha institucionalizado el monitoreo del control interno. Se han desarrollado políticas y procedimientos para evaluar y reportar las actividades de monitoreo del control interno. Se ha definido un programa de educación y entrenamiento para el monitoreo del control interno. Se ha definido también un proceso para auto-evaluaciones y revisiones de aseguramiento del control interno, con roles definidos para los responsables de la administración del negocio y de TI. Se usan herramientas, aunque no necesariamente están integradas en todos los procesos. Las políticas de evaluación de riesgos de los procesos de TI se utilizan dentro de los marcos de trabajo desarrollados de manera específica para la función de TI. Se han definido políticas para el manejo y mitigación de riesgos específicos de procesos.

• Nivel 4: Administrado y Medible

Cuando la gerencia tiene implantado un marco de trabajo para el monitoreo del control interno de TI. La organización ha establecido niveles de tolerancia para el proceso de monitoreo del control interno. Se han implantado herramientas para estandarizar evaluaciones para detectar de forma automática las excepciones de control. Se ha establecido una función formal para el control interno de TI, con profesionales especializados y certificados que utilizan un marco de trabajo de control formal avalado por la alta dirección. Un equipo calificado de TI participa de forma rutinaria en las evaluaciones de control interno. Se ha establecido una base de datos de métricas para información histórica sobre el monitoreo del control interno. Se realizan revisiones entre pares para verificar el monitoreo del control interno.

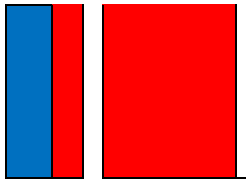
• Nivel 5: Optimizado

Cuando la gerencia tiene implantado un marco de trabajo para el monitoreo del control interno de TI. La organización ha establecido niveles de tolerancia para el proceso de monitoreo del control interno. Se han implantado herramientas para estandarizar evaluaciones y para detectar de forma automática las excepciones del control. Se ha establecido una función formal para el control interno de TI, con profesionales especializados y certificados que utilizan un marco de trabajo de control formal avalado por la alta dirección. Un equipo calificado de TI participa de forma rutinaria en las evaluaciones de control interno. Se realizan revisiones entre pares para verificar el monitoreo del control interno.

## 2. Criterios de Evaluación

Bajo los siguientes criterios se optó por revisar cada uno de los controles de seguridad identificados en la Declaración de Aplicabilidad – SOA.

| NIVEL DE MADUREZ | Existencia | Documentación | Actividades | Formalización | Divulgación | Prueba de Recorrido | Asignación | Indicadores | Monitoreo | Naturaleza | Práctica Líder |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 5 | Si | Completa | Secuencia adecuada | Si | Partes interesadas | Si | Nivel táctico o Nivel Ejecutivo | Medidos o Gestionados | Administrado o Gestionado | Semiautomático, Automático o Manual | Si |
| 4 | Si | Completa | Secuencia adecuada | Si | Partes interesadas | Si | | Medidos o Gestionados | Administrado o Gestionado | | |
| 3 | Si | Completa | Secuencia adecuada | Si | Partes interesadas | Si | | | | | |
| 2 | Si | Completa o Incompleta | Secuencia adecuada o Secuencia informal | | | | | | | | |
| 1 | Si | Completa o Incompleta | | | | | | | | | |
| 0 | No | | | | | | | | | | |



## 3. Evaluación Controles de Seguridad

A continuación se presentan los resultados sobre los controles de seguridad:

### 5. Políticas de Seguridad

| DESCRIPCION CONTROL | Control | EXISTENCIA | DOCUMENTACIÓN | ACTIVIDADES | FORMALIZACIÓN | DIVULGACIÓN | PRUEBA RECORRIDO | ASIGNACIÓN | INDICADORES | MONITOREO | NATURALEZA | PRÁCTICA LIDER |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Política de Seguridad de la Información** | | | | | | | | | | | | |
| **Políticas para la seguridad de la información** | Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los emplea | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | dos y a las partes externas pertinentes. | | | | | | | | | | | |
| **Revisión de las políticas para la seguridad de la información** | Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas. | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

## 6. Organización de la Seguridad

| DESCRIPCION CONTROL | Control | EXISTENCIA | DOCUMENTACIÓN | ACTIVIDADES | FORMALIZACIÓN | DIVULGACIÓN | PRUEBA RECORRIDO | ASIGNACIÓN | INDICADORES | MONITOREO | NATURALEZA | PRÁCTICA LIDER |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Organización Interna** | | | | | | | | | | | | |
| **Roles y responsabilidades para la seguridad de la información** | Se deben definir y asignar todas las responsabilidades de la seguridad de la información. | SI | NO | SI | NO | NO | NO | NO | NO | NO | MANUAL | NO |
| **Separación de deberes** | Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización. | SI | NO | SI | NO | NO | NO | NO | NO | NO | MANUAL | NO |
| **Contacto con las Autoridades** | Se deben mantener contactos apropiados | SI | NO | SI | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | con las autoridades pertinentes. | | | | | | | | | | | |
| **Contacto con Grupos de Interés especial** | Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad. | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |
| **Seguridad de la información en gestión de proyectos** | La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto. | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |
| **Dispositivos móviles y teletrabajo** | | | | | | | | | | | | |
| **Política para dispositivos móviles** | Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | por el uso de dispositivos móviles. | | | | | | | | | | | |
| **Teletrabajo** | Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo. | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

## 7. Recursos Humanos

| DESCRIPCION CONTROL | Control | EXISTENCIA | DOCUMENTACIÓN | ACTIVIDADES | FORMALIZACIÓN | DIVULGACIÓN | PRUEBA RECORRIDO | ASIGNACIÓN | INDICADORES | MONITOREO | NATURALEZA | PRÁCTICA LIDER |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Antes de asumir el empleo** | | | | | | | | | | | | |
| **Selección** | Las verificaciones de los antecedentes de todos los candidatos a un | SI | SI | SI | SI | SI | SI | SI | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos. | | | | | | | | | | | |
| **Términos y condiciones del empleo** | Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organizaci | SI | SI | SI | SI | SI | SI | SI | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ón en cuanto a la seguridad de la información. | | | | | | | | | | | |
| **Durante la ejecución del empleo** | | | | | | | | | | | | |
| **Responsabilidades de la dirección** | La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización. | SI | SI | SI | SI | SI | SI | SI | NO | NO | MANUAL | NO |
| **Toma de conciencia, educación y formación en la seguridad de la información** | Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo. | | | | | | | | | | | |
| **Proceso disciplinario** | Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información | SI | NO | SI | NO | NO | SI | SI | NO | NO | MANUAL | NO |
| **Terminación y cambio de empleo** | | | | | | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Terminación o cambio de responsabilidades de empleo** | Las responsabilidades y los deberes de la información que permanecen validos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir. | SI | SI | SI | NO | NO | SI | SI | NO | NO | MANUAL | NO |

## 8. Gestión de Activos

| DESCRIPCION CONTROL | Control | EXISTENCIA | DOCUMENTACIÓN | ACTIVIDADES | FORMALIZACIÓN | DIVULGACIÓN | PRUEBA RECORRIDO | ASIGNACIÓN | INDICADORES | MONITOREO | NATURALEZA | PRÁCTICA LIDER |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Responsabilidad por los activos** | | | | | | | | | | | | |
| **Inventario de activos** | Se deben identificar los activos asociados con la informaci | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ón e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos. | | | | | | | | | | | |
| **Propiedad de los activos** | Los activos mantenidos en el inventario deben tener un propietario. | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |
| **Uso aceptable de los activos** | Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos | SI | NO | SI | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | asociados con información e instalaciones de procesamiento de información. | | | | | | | | | | | |
| **Devolución de activos** | Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo. | SI | NO | SI | NO | NO | NO | NO | NO | NO | MANUAL | NO |
| **Clasificación de la información** | | | | | | | | | | | | |
| **Clasificación de la información** | La información se debe clasificar en | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. | | | | | | | | | | | |
| **Etiquetado de la información** | Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | organización. | | | | | | | | | | | |
| **Manejo de activos** | Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización. | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |
| **Manejo de medios de soporte** | | | | | | | | | | | | |
| **Gestión de medios removibles** | Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el | NO | NO | NO | NO | NO | NO | NO | NO | NO | SEMIAUTOMÁTICO | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | esquema de clasificación adoptado por la organización. | | | | | | | | | | | |
| **Disposición de los medios** | Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales. | NO | NO | NO | NO | NO | NO | NO | NO | NO | SEMIAUTOMÁTICO | NO |
| **Transferencia de medios físicos** | Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | transporte. | | | | | | | | | | | |

## 9. Control de Acceso

| DESCRIPCION CONTROL | Control | EXISTENCIA | DOCUMENTACIÓN | ACTIVIDADES | FORMALIZACIÓN | DIVULGACIÓN | PRUEBA RECORRIDO | ASIGNACIÓN | INDICADORES | MONITOREO | NATURALEZA | PRÁCTICA LIDER |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Requisitos del negocio para control de acceso** | | | | | | | | | | | | |
| **Política de control de acceso** | Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |
| **Acceso a redes y a servicios en red** | Solo se debe permitir acceso de los usuarios a la | SI | NO | SI | NO | SI | SI | NO | NO | NO | SEMIAUTOMÁTICO | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | red y a los servicios de red para los que hayan sido autorizados específicamente. | | | | | | | | | | | |
| **Gestión de acceso de usuarios** | | | | | | | | | | | | |
| **Registro y cancelación del registro de usuarios** | Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. | SI | NO | SI | NO | NO | SI | NO | NO | NO | SEMIAUTOMÁTICO | NO |
| **Suministro de acceso de usuarios** | Se debe implementar un proceso de suminist | SI | NO | SI | NO | NO | SI | NO | NO | NO | SEMIAUTOMÁTICO | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios. | | | | | | | | | | | |
| **Gestión de derechos de acceso privilegiado** | Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. | SI | NO | SI | NO | NO | SI | NO | NO | NO | SEMIAUTOMÁTICO | NO |
| **Gestión de información de autenticación secreta de usuarios** | La asignación de información de | SI | NO | SI | NO | NO | SI | NO | NO | NO | SEMIAUTOMÁTICO | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | autenticación secreta se debe controlar por medio de un proceso de gestión formal. | | | | | | | | | | | |
| **Revisión de los derechos de acceso de usuarios** | Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares. | NO | NO | NO | NO | NO | NO | NO | NO | NO | SEMIAUTOMÁTICO | NO |
| **Cancelación o ajuste de los derechos de acceso** | Los derechos de acceso de todos los empleados y de usuarios | SI | NO | SI | NO | NO | SI | NO | NO | NO | SEMIAUTOMÁTICO | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios. | | | | | | | | | | | |
| **Responsabilidades de los usuarios** | | | | | | | | | | | | |
| **Uso de información de autenticación secreta** | Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | información de autenticación secreta. | | | | | | | | | | | |
| **Control de acceso a sistemas y aplicaciones** | | | | | | | | | | | | |
| **Restricción de acceso a información** | El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso. | NO | NO | NO | NO | NO | NO | NO | NO | NO | AUTOMÁTICO | NO |
| **Procedimiento de conexión segura** | Cuando lo requiere la política de control de acceso, el acceso a sistema | NO | NO | NO | NO | NO | NO | NO | NO | NO | SEMIAUTOMÁTICO | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | s y aplicaciones se debe controlar mediante un proceso de ingreso seguro. | | | | | | | | | | | |
| **Sistema de gestión de contraseñas** | Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas. | NO | NO | NO | NO | NO | NO | NO | NO | NO | SEMIAUTOMÁTICO | NO |
| **Uso de programas utilitarios privilegiados** | Se debe restringir y controlar estrictamente el uso de programas utilitario | NO | NO | NO | NO | NO | NO | NO | NO | NO | SEMIAUTOMÁTICO | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | s que podrían tener capacidad de anular el sistema y los controles de las aplicaciones. | | | | | | | | | | | |
| **Control de acceso a códigos fuente de programas** | Se debe restringir el acceso a los códigos fuente de los programas. | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

## 10. Criptografía

| DESCRIPCION CONTROL | Control | EXISTENCIA | DOCUMENTACIÓN | ACTIVIDADES | FORMALIZACIÓN | DIVULGACIÓN | PRUEBA RECORRIDO | ASIGNACIÓN | INDICADORES | MONITOREO | NATURALEZA | PRÁCTICA LIDER |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Política sobre el uso de controles criptográficos** | Se debe desarrollar e implementar una política sobre el uso | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | de controles criptográficos para la protección de la información | | | | | | | | | | | |
| **Gestión de claves** | Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida. | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

## 11. Seguridad Física

| DESCRIPCION CONTROL | Control | EXISTENCIA | DOCUMENTACIÓN | ACTIVIDADES | FORMALIZACIÓN | DIVULGACIÓN | PRUEBA RECO | ASIGNACIÓN | INDICADORES | MONITOREO | NATURALEZA | PRÁCTICA |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | RRIDO | | | | | LIDER |
| **Áreas seguras** | | | | | | | | | | | | |
| **Perímetro de seguridad física** | Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información. | SI | NO | SI | NO | NO | SI | SI | NO | NO | MANUAL | NO |
| **Controles de acceso físicos** | Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a | SI | NO | SI | NO | NO | SI | SI | NO | NO | SEMIAUTOMÁTICO | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | personal autorizado. | | | | | | | | | | | |
| **Seguridad de oficinas, recintos e instalaciones** | Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones. | SI | NO | SI | NO | NO | SI | SI | NO | NO | SEMIAUTOMÁTICO | NO |
| **Protección contra amenazas externas y ambientales** | Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. | SI | NO | SI | NO | NO | SI | SI | NO | NO | SEMIAUTOMÁTICO | NO |
| **Trabajo en áreas seguras** | Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras. | SI | NO | SI | NO | NO | SI | SI | NO | NO | MANUAL | NO |
| **Áreas de despacho y carga** | Se deben controlar los puntos de acceso tales como áreas de | NO | NO | NO | NO | NO | NO | NO | NO | NO | SEMIAUTOMÁTICO | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado. | | | | | | | | | | | |
| **Equipos** | | | | | | | | | | | | |
| **Ubicación y protección de los equipos** | Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros | SI | NO | SI | NO | NO | SI | SI | NO | NO | SEMIAUTOMÁTICO | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | del entorno, y las posibilidades de acceso no autorizado. | | | | | | | | | | | |
| **Servicios de suministro** | Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | SI | NO | SI | NO | NO | SI | SI | NO | NO | SEMIAUTOMÁTICO | NO |
| **Seguridad del cableado** | El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de | SI | NO | SI | NO | NO | NO | SI | NO | NO | SEMIAUTOMÁTICO | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | información se debe proteger contra intercepta ción, interferen cia o daño. | | | | | | | | | | | |
| **Mantenimiento de equipos** | Los equipos se deben mantener correctam ente para asegurar su disponibili dad e integridad continuas . | SI | NO | SI | SI | NO | SI | SI | NO | NO | SEMIAUT OMÁTIC O | NO |
| **Retiro de activos** | Los equipos, informaci ón o software no se deben retirar de su sitio sin autorizaci ón previa. | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |
| **Seguridad de equipos y activos fuera de las instalaciones** | Se deben aplicar medidas de seguridad a los activos | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones. | | | | | | | | | | | |
| **Disposición segura o reutilización de equipos** | Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | sobrescrito en forma segura antes de su disposición o reúso. | | | | | | | | | | | |
| **Equipos de usuario desatendido** | Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada. | SI | NO | SI | NO | NO | SI | NO | NO | NO | SEMIAUTOMÁTICO | NO |
| **Política de escritorio limpio y pantalla limpia** | Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las | SI | NO | SI | NO | NO | SI | NO | NO | NO | SEMIAUTOMÁTICO | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | instalaciones de procesamiento de información. | | | | | | | | | | | |

## 12. Seguridad de Operaciones

| DESCRIPCION CONTROL | Control | EXISTENCIA | DOCUMENTACIÓN | ACTIVIDADES | FORMALIZACIÓN | DIVULGACIÓN | PRUEBA RECORRIDO | ASIGNACIÓN | INDICADORES | MONITOREO | NATURALEZA | PRÁCTICA LIDER |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Procedimientos operacionales y responsabilidades** | | | | | | | | | | | | |
| **Procedimientos de operación documentados** | Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan. | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |
| **Gestión de cambios** | Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | los sistemas de procesamiento de información que afectan la seguridad de la información. | | | | | | | | | | | |
| **Gestión de capacidad** | Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema. | SI | NO | SI | NO | NO | NO | SI | NO | SI | AUTOMÁTICO | NO |
| **Separación de los ambientes de desarrollo, pruebas,** | Se deben separar los ambientes de desarrollo, prueba y | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **y operación** | operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación. | | | | | | | | | | | |
| **Protección contra códigos maliciosos** | | | | | | | | | | | | |
| **Controles contra códigos maliciosos** | Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos. | SI | NO | SI | NO | NO | SI | SI | NO | SI | SEMIAUTOMÁTICO | NO |
| **Copias de respaldo** | | | | | | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Respaldo de la información** | Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. | SI | NO | SI | NO | NO | SI | SI | NO | SI | AUTOMÁTICO | NO |
| **Registro y seguimiento** | | | | | | | | | | | | |
| **Registro de eventos** | Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la | NO | NO | NO | NO | NO | NO | NO | NO | NO | AUTOMÁTICO | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | informaci ón. | | | | | | | | | | | |
| **Protecció n de la informaci ón de registro** | Las instalacio nes y la informaci ón de registro se deben proteger contra alteración y acceso no autorizad o. | NO | NO | NO | NO | NO | NO | NO | NO | NO | AUTOMÁTI CO | NO |
| **Registros del administr ador y del operador** | Las actividade s del administr ador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularida d. | NO | NO | NO | NO | NO | NO | NO | NO | NO | AUTOMÁTI CO | NO |
| **Sincroniz ación de relojes** | Los relojes de todos los sistemas de procesam iento de informaci | SI | NO | SI | NO | NO | SI | SI | NO | NO | AUTOMÁTI CO | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ón pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo. | | | | | | | | | | | |
| **Control de software operacional** | | | | | | | | | | | | |
| **Instalación de software en sistemas operativos** | Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos. | SI | NO | SI | NO | NO | SI | SI | NO | NO | AUTOMÁTICO | NO |
| **Gestión de la Vulnerabilidad Técnica** | | | | | | | | | | | | |
| **Gestión de las vulnerabilidades técnicas** | Se debe obtener oportunamente información acerca de las vulnerabilidades | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. | | | | | | | | | | | |
| **Restricciones sobre la instalación de software** | Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios. | SI | NO | SI | NO | NO | SI | SI | NO | NO | AUTOMÁTICO | NO |
| **Consideraciones sobre auditorías de sistemas de información** | | | | | | | | | | | | |
| **Controles de auditorías de sistemas de** | Los requisitos y actividades de auditoria | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **información** | que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio. | | | | | | | | | | | |

## 13. Seguridad de Comunicaciones

| DESCRIPCION CONTROL | Control | EXISTENCIA | DOCUMENTACIÓN | ACTIVIDADES | FORMALIZACIÓN | DIVULGACIÓN | PRUEBA RECORRIDO | ASIGNACIÓN | INDICADORES | MONITOREO | NATURALEZA | PRÁCTICA LIDER |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Gestión de seguridad de redes** | | | | | | | | | | | | |
| **Controles de redes** | Las redes se deben gestionar y controlar para proteger la información en sistemas | SI | NO | SI | NO | NO | NO | SI | NO | NO | SEMIAUTOMÁTICO | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | y aplicaciones | | | | | | | | | | | |
| **Seguridad de los servicios de red** | Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente. | SI | NO | SI | NO | NO | NO | SI | NO | NO | AUTOMÁTICO | NO |
| **Separación en las redes** | Los grupos de servicios de información, | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | usuarios y sistemas de información se deben separar en las redes. | | | | | | | | | | | |
| **Transferencia de información** | | | | | | | | | | | | |
| **Políticas y procedimientos de transferencia de información** | Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones. | SI | NO | SI | NO | NO | NO | SI | NO | NO | MANUAL | NO |
| **Acuerdos sobre transferencia de** | Los acuerdos deben tratar la transferen | SI | SI | SI | SI | NO | NO | SI | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **información** | cia segura de información del negocio entre la organización y las partes externas. | | | | | | | | | | | |
| **Mensajería electrónica** | Se debe proteger adecuadamente la información incluida en la mensajería electrónica | SI | NO | SI | NO | NO | NO | SI | NO | NO | SEMIAUTOMÁTICO | NO |
| **Acuerdos de confidencialidad o de no divulgación** | Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la | SI | NO | SI | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | organización para la protección de la información. | | | | | | | | | | | |

## 14. Desarrollo de Software

| DESCRIPCION CONTROL | Control | EXISTENCIA | DOCUMENTACIÓN | ACTIVIDADES | FORMALIZACIÓN | DIVULGACIÓN | PRUEBA RECORRIDO | ASIGNACIÓN | INDICADORES | MONITOREO | NATURALEZA | PRÁCTICA LIDER |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Requisitos de seguridad de los sistemas de información** | | | | | | | | | | | | |
| **Análisis y especificación de requisitos de seguridad de la información** | Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes. | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Seguridad de servicios de las aplicaciones en redes públicas** | La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas. | NO | NO | NO | NO | NO | NO | NO | NO | NO | SEMIAUTOMÁTICO | NO |
| **Protección de transacciones de servicios de las aplicaciones** | La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada. | | | | | | | | | | | |
| **Seguridad en los procesos de desarrollo y de soporte** | | | | | | | | | | | | |
| **Política de desarrollo seguro** | Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | organización. | | | | | | | | | | | |
| **Procedimientos de control de cambios en sistemas** | Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios. | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| **Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones** | Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | operaciones o seguridad de la organización. | | | | | | | | | | | |
| **Restricciones sobre cambios en los paquetes de software** | Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente. | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| **Principios de organización de sistemas seguros** | Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | actividad de implementación de sistemas de información. | | | | | | | | | | | |
| **Ambiente de desarrollo seguro** | Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas. | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| **Desarrollo contratado externamente** | La organización debe supervisar y hacer seguimien | SI | NO | SI | NO | NO | SI | SI | NO | SI | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | to de la actividad de desarrollo de sistemas contratados externamente. | | | | | | | | | | | |
| **Pruebas de seguridad de sistemas** | Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad. | SI | NO | SI | NO | NO | SI | SI | NO | SI | SEMIAUTOMÁTICO | NO |
| **Prueba de aceptación de sistemas** | Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación | SI | NO | SI | NO | NO | SI | SI | NO | SI | SEMIAUTOMÁTICO | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | relacionados. | | | | | | | | | | | |
| **Datos de ensayo** | | | | | | | | | | | | |
| **Protección de datos de ensayo** | Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente. | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

## 15. Terceras Partes

| DESCRIPCION CONTROL | Control | EXISTENCIA | DOCUMENTACIÓN | ACTIVIDADES | FORMALIZACIÓN | DIVULGACIÓN | PRUEBA RECORRIDO | ASIGNACIÓN | INDICADORES | MONITOREO | NATURALEZA | PRÁCTICA LIDER |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Seguridad de la información en las relaciones con los proveedores** | | | | | | | | | | | | |
| **Política de seguridad de la información para las relaciones con proveedores** | Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | acordar con estos y se deben documentar | | | | | | | | | | | |
| **Tratamiento de la seguridad dentro de los acuerdos con proveedores** | Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización. | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Cadena de suministro de tecnología de información y comunicación** | Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación. | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |
| **Gestión de la prestación de servicios de proveedores** | | | | | | | | | | | | |
| **Seguimiento y revisión de los servicios de los proveedores** | Las organizaciones deben hacer seguimiento, revisar y auditar | SI | NO | SI | NO | NO | NO | SI | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | con regularidad la prestación de servicios de los proveedores | | | | | | | | | | | |
| **Gestión de cambios a los servicios de los proveedores** | Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos. | | | | | | | | | | | |

## 16. Incidentes de Seguridad

| DESCRIPCION CONTROL | Control | EXISTENCIA | DOCUMENTACIÓN | ACTIVIDADES | FORMALIZACIÓN | DIVULGACIÓN | PRUEBA RECORRIDO | ASIGNACIÓN | INDICADORES | MONITOREO | NATURALEZA | PRÁCTICA LIDER |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Gestión de incidentes y mejoras en la seguridad de la información** | | | | | | | | | | | | |
| **Responsabilidades y procedimientos** | Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | de la información. | | | | | | | | | | | |
| **Reporte de eventos de seguridad de la información** | Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible. | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |
| **Reporte de debilidades de seguridad de la información** | Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | de la información observada o sospechada en los sistemas o servicios. | | | | | | | | | | | |
| **Evaluación de eventos de seguridad de la información y decisiones sobre ellos** | Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información. | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |
| **Respuesta a incidentes de seguridad de la información** | Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimi | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | entos documentados. | | | | | | | | | | | |
| **Aprendizaje obtenido de los incidentes de seguridad de la información** | El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros. | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |
| **Recolección de evidencia** | La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda | NO | NO | NO | NO | NO | NO | NO | NO | NO | SEMIATOMÁTICO | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | servir como evidencia. | | | | | | | | | | | |

## 17. Continuidad de Negocio

| DESCRIPCION CONTROL | Control | EXISTENCIA | DOCUMENTACIÓN | ACTIVIDADES | FORMALIZACIÓN | DIVULGACIÓN | PRUEBA RECORRIDO | ASIGNACIÓN | INDICADORES | MONITOREO | NATURALEZA | PRÁCTICA LIDER |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Continuidad de seguridad de la información** | | | | | | | | | | | | |
| **Planificación de la continuidad de la seguridad de la información** | La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | adversas, por ejemplo, durante una crisis o desastre. | | | | | | | | | | | |
| **Implementación de la continuidad de la seguridad de la información** | La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | información durante una situación adversa. | | | | | | | | | | | |
| **Verificación, revisión y evaluación de la continuidad de la seguridad de la información** | La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficace | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | s durante situaciones adversas. | | | | | | | | | | | |
| **Redundancias** | | | | | | | | | | | | |
| **Disponibilidad de instalaciones de procesamiento de información** | Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad. | NO | NO | NO | NO | NO | NO | NO | NO | NO | SEMIAUTOMÁTICO | NO |

## 18. Cumplimiento

| DESCRIPCION CONTROL | Control | EXISTENCIA | DOCUMENTACIÓN | ACTIVIDADES | FORMALIZACIÓN | DIVULGACIÓN | PRUEBA RECORRIDO | ASIGNACIÓN | INDICADORES | MONITOREO | NATURALEZA | PRÁCTICA LIDER |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Cumplimiento de requisitos legales y contractuales** | | | | | | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Identificación de los requisitos de la legislación aplicable y de los requisitos contractuales** | Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización. | SI | NO | SI | NO | NO | SI | SI | NO | NO | MANUAL | NO |
| **Derechos de propiedad intelectual** | Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y | SI | NO | SI | NO | NO | SI | SI | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. | | | | | | | | | | | |
| **Protección de registros** | Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio. | SI | NO | SI | NO | NO | NO | SI | NO | NO | SEMIAUTOMÁTICO | NO |
| **Privacidad y protección de información de datos** | Se deben asegurar la privacidad y protección de la información de datos | SI | NO | SI | NO | NO | SI | SI | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **personales** | personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable. | | | | | | | | | | | |
| **Reglamentación de controles criptográficos** | Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes. | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| **Revisiones de seguridad de la información** | | | | | | | | | | | | |
| **Revisión independiente de la seguridad de la información** | El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | procesos y los procedimientos para seguridad de la información ) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos. | | | | | | | | | | | |
| **Cumplimiento con las políticas y normas de seguridad** | Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | requisito de seguridad. | | | | | | | | | | | |
| **Revisión del cumplimiento técnico** | Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información. | NO | NO | NO | NO | NO | NO | NO | NO | NO | MANUAL | NO |

## 4. Referencias

[1] C. 4. D. d. a. (. ©. 2007, «COBIT® 4.1,» de *CobiT4.1 Marco de Trabajo Objetivos de Control Directrices Gerenciales Modelos de Madurez*, Rolling Meadows, IL 60008 EE.UU., IT Governance Institute, 2007, p. 168.