Instalación desprotegida
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
11.2.3 Seguridad del cableado

Uso no aceptable de activos
7.2.2 Concienciación, educación y capacitación de la seguridad de la información
7.2.3 Proceso disciplinario
8.1.3 Uso aceptable de los activos

Susceptibilidad a polvo, humedad.
11.1.4 Protección contra amenazas externas y ambientales
11.2.1 Ubicación y protección de equipos

Gestión inadecuada de terceras partes
15.1.1 Política de seguridad en la relación con proveedores
15.1.2 Seguridad en el acuerdo con proveedores
15.1.3 Tecnología de la información y comunicacion en la cadena de suministro

No existe concienciación y formación en seguridad
7.2.1 Responsabilidades de la dirección
7.2.2 Concienciación, educación y capacitación de la seguridad de la información

No existe supervisión de terceros dentro de la organización
11.1.3 Seguridad de oficinas, salas e instalaciones

Proceso de contratación ineficiente
7.1.2 Términos y condiciones del puesto de trabajo
15.2.2 Gestión de cambios en la provisión de servicios

Exposición a temperaturas extremas
11.1.4 Protección contra amenazas externas y ambientales

No existe sistema estabilizador de tensión
11.2.2 Servicios de suministro

Uso incorrecto de equipos
7.2.2 Concienciación, educación y capacitación de la seguridad de la información
8.1.3 Uso aceptable de los activos
11.2.6 Seguridad de equipos y activos fuera de las instalaciones

Mantenimiento insuficiente	Gestión de cambios ineficiente
11.2.4 Mantenimiento de equipos	12.1.2 Gestión del cambio

Mantenimiento insuficiente	No existe gestión de activos
11.2.4 Mantenimiento de equipos	8.1.1 Inventario de activos
	8.1.2 Propiedad de los activos
	8.1.3 Uso aceptable de los activos

Planificación y monitorización de capacidad inadecuada
12.1.3 Gestión de la capacidad

No existen equipos de detección de incendios
11.1.3 Seguridad de oficinas, salas e instalaciones

No existen equipos de extinción de incendios
11.1.4 Protección contra amenazas externas y ambientales

Ubicaciones suceptibles a inundación
11.1.3 Seguridad de oficinas, salas e instalaciones
11.1.4 Protección contra amenazas externas y ambientales
11.2.1 Ubicación y protección de equipos

No existe control de los activos fuera de las instalaciones	No existe gestión de activos
11.2.5 Retirada de activos	8.1.1 Inventario de activos
11.2.6 Seguridad de equipos y activos fuera de las instalaciones	8.1.2 Propiedad de los activos
	8.1.3 Uso aceptable de los activos
	8.1.4 Devolución de los activos

No existe procedimiento para el control de cambios
12.1.2 Gestión del cambio

No existen políticas para el uso de dispositivos portátiles	Uso no aceptable de activos
6.2.1 Política de dispositivos móviles	8.1.3 Uso aceptable de los activos

Exposición a humedad, polvo, suciedad	No existe gestión de activos
11.1.4 Protección contra amenazas externas y ambientales	8.1.1 Inventario de activos
11.2.1 Ubicación y protección de equipos	8.1.2 Propiedad de los activos
11.2.4 Mantenimiento de equipos	8.1.3 Uso aceptable de los activos

No existen procedimiento para devolución de activos
8.1.4 Devolución de los activos
8.3.1 Gestión de medios removibles

Instalación desprotegida	No existe gestión de activos
11.1.1 Perímetro de seguridad física	8.1.1 Inventario de activos
11.1.2 Controles de acceso físico	8.1.2 Propiedad de los activos
11.1.3 Seguridad de oficinas, salas e instalaciones	
11.1.6 Áreas de entrega y carga	
11.2.1 Ubicación y protección de equipos	

No existen políticas para el uso de dispositivos portátiles
6.2.1 Política de dispositivos móviles
11.2.5 Retirada de activos
11.2.6 Seguridad de equipos y activos fuera de las instalaciones

No existen procedimiento para devolución de activos	Acceso remoto no seguro
8.1.4 Devolución de los activos	9.1.2 Acceso a redes y servicios de red

Conexiones a red pública desprotegidas	Eliminación o reutilizacion de soportes sin borrar
13.1.1 Controles de red	8.3.1 Gestión de medios removibles
13.1.2 Seguridad de servicios de red	8.3.2 Desecho de medios
13.1.3 Segregación de redes	

Gestión del control de acceso ineficiente
9.4.1 Restricción del acceso a la información

No existen mecanismos de autenticación y validación del usuario
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
9.2.5 Revisión de los derechos de acceso de usuarios

No existen procedimientos formales para alta y baja de usuarios
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	Cableado desprotegido
8.1.1 Inventario de activos	11.2.3 Seguridad del cableado
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	

Comunicaciones a través de redes públicas o desprotegidas
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
12.2.1 Controles contra código malicioso

No existen procedimientos de monitorización de las instalaciones
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

No existe control sobre el uso de utilidades de sistema
12.7.1 Controles de la auditoría de sistemas de información

No existen registros de auditoría
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

No existe protección contra código malicioso
12.2.1 Controles contra código malicioso
12.3.1 Copia de seguridad de la información

No existe concienciación y formación en seguridad
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
7.2.3 Proceso disciplinario

Uso no aceptable de activos
8.1.3 Uso aceptable de los activos

Comunicaciones a través de redes públicas o desprotegidas
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
8.3.1 Gestión de medios removibles
12.1.4 Separación de entornos de desarrollo, prueba y operación
12.3.1 Copia de seguridad de la información

No existen procedimientos de autorización para la información pública
14.1.2 Seguridad del servicio de aplicacion en redes públicas

No existen procedimientos para el etiquetado y manejo de la información
8.2.1 Clasificación de la información
8.2.2 Etiquetado de la información
8.2.3 Manejo de activos

Control de acceso al edificio y a las salas ineficiente
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
11.1.1 Perímetro de seguridad física

Eliminación o reutilizacion de soportes sin borrar
8.1.4 Devolución de los activos
8.3.2 Desecho de medios
11.2.7 Seguridad en el desecho o reutilización de equipos

No existe control para copia de información
6.2.2 Teletrabajo
8.3.1 Gestión de medios removibles
8.3.3 Tránsito de medios físicos
12.3.1 Copia de seguridad de la información
12.4.1 Registro de eventos

No existe concienciación y formación en seguridad
7.2.1 Responsabilidades de la dirección
7.2.2 Concienciación, educación y capacitación de la seguridad de la información

No existen acuerdos de confidencialidad
7.2.1 Responsabilidades de la dirección
13.2.4 Acuerdos de confidencialidad y no divulgación

No existen políticas para el correcto uso de telecomunicaciones
8.1.3 Uso aceptable de los activos

No existen políticas para el uso de dispositivos portátiles
6.2.1 Política de dispositivos móviles
6.2.2 Teletrabajo
11.2.6 Seguridad de equipos y activos fuera de las instalaciones

No existen procedimientos para la comunicación de incidentes de seguridad de la información
16.1.1 Responsabilidades y procedimientos
16.1.2 Reporte de eventos sobre la seguridad de la información
16.1.3 Reporte de debilidades en la seguridad de la información

No existe asignación de responsablidades relacionadas a la seguridad de la información
6.1.1 Roles y responsabilidades de la seguridad de la información
7.2.1 Responsabilidades de la dirección

No existe separación de funciones	Personal clave de seguridad no disponible
6.1.2 Segregación de tareas	12.1.3 Gestión de la capacidad

Proceso de contratación ineficiente
7.1.1 Selección
7.1.2 Términos y condiciones del puesto de trabajo
7.3.1 Finalización o cambios en las responsabilidades del puesto de trabajo

Gestión inadecuada de terceras partes
15.1.2 Seguridad en el acuerdo con proveedores

No existen auditorías regulares
18.2.1 Revisión independiente de la seguridad de la información
18.2.2 Cumplimiento de politicas y normas de seguridad
18.2.3 Revisión de cumplimiento técnico

No existen procedimientos para cumplimiento de la propiedad intelectual
18.1.2 Derechos de propiedad intelectual

No existen requisitos de seguridad en contratos de empleados
6.1.1 Roles y responsabilidades de la seguridad de la información
7.1.2 Términos y condiciones del puesto de trabajo
7.2.1 Responsabilidades de la dirección

Violación de la legislación aplicable
18.1.1 Identificación de legislación aplicable y requisitos contractuales
18.1.4 Privacidad y protección de información de identificación personal
18.1.5 Regulación de controles de criptografía
18.2.2 Cumplimiento de politicas y normas de seguridad
18.2.3 Revisión de cumplimiento técnico

Gestión del control de acceso ineficiente
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
9.2.5 Revisión de los derechos de acceso de usuarios
9.2.6 Retirada o ajuste de los derechos de acceso

No existe política de puesto de trabajo y pantallas limpias
11.2.8 Equipos de usuario desatendido
11.2.9 Política de pantalla y escritorio despejado

No existe supervisión de los empleados que trabajan fuera de horario de oficina
9.4.2 Procesos de inicio seguro de sesión
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

No existe supervisión de terceros dentro de la organización
11.1.5 Trabajo en áreas seguras
11.1.6 Áreas de entrega y carga
13.2.4 Acuerdos de confidencialidad y no divulgación
15.1.2 Seguridad en el acuerdo con proveedores

No existen mecanismos de monitorización
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

No existen procedimiento para eliminar permisos de acceso
7.3.1 Finalización o cambios en las responsabilidades del puesto de trabajo
9.2.3 Gestión de derechos de acceso privilegiado
9.2.5 Revisión de los derechos de acceso de usuarios
9.2.6 Retirada o ajuste de los derechos de acceso

No existe control de los activos fuera de las instalaciones
6.2.1 Política de dispositivos móviles
6.2.2 Teletrabajo
11.2.6 Seguridad de equipos y activos fuera de las instalaciones

No existen procedimiento para devolución de activos
8.1.1 Inventario de activos
8.1.2 Propiedad de los activos
8.1.4 Devolución de los activos

No existen procesos disciplinarios claros para incidentes de seguridad de la información
7.2.3 Proceso disciplinario

Gestión de políticas de seguridad de la información insuficiente
5.1.1 Políticas para la seguridad de la información
5.1.2 Revisión de las políticas para la seguridad de la información
6.1.5 Seguridad de la información en la gestión de proyectos
18.2.2 Cumplimiento de politicas y normas de seguridad

No existe contacto con otras organizaciones y grupos de interés
6.1.3 Contacto con las autoridades
6.1.4 Contacto con grupos de interés especial

No existe documentacion
12.1.1 Procedimientos operativos documentados

No existe plan de continuidad
17.1.1 Planificacion de la continuidad de la seguridad de la información
17.1.2 Implementación de la continuidad de la seguridad de la información
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información
17.2.1 Disponibilidad de las instalaciones de procesamiento de información

No existe procedimiento para la gestión de incidencias de seguridad
16.1.1 Responsabilidades y procedimientos
16.1.2 Reporte de eventos sobre la seguridad de la información
16.1.3 Reporte de debilidades en la seguridad de la información
16.1.4 Valoración y decisión sobre los eventos de seguridad de la información
16.1.5 Respuesta a los incidentes de seguridad de la información
16.1.6 Aprendizaje de los incidentes de seguridad de la información
16.1.7 Recolección de evidencias

No existen auditorías regulares
18.2.1 Revisión independiente de la seguridad de la información
18.2.2 Cumplimiento de politicas y normas de seguridad
18.2.3 Revisión de cumplimiento técnico

Violación de la legislación aplicable
18.1.1 Identificación de legislación aplicable y requisitos contractuales
18.1.2 Derechos de propiedad intelectual
18.1.3 Protección de registros
18.1.4 Privacidad y protección de información de identificación personal
18.1.5 Regulación de controles de criptografía

Gestión de red ineficiente	No existe procedimiento para el control de cambios
13.1.1 Controles de red	15.2.2 Gestión de cambios en la provisión de servicios
13.1.2 Seguridad de servicios de red	
13.1.3 Segregación de redes	

No existen acuerdos de calidad de servicio (SLA)
15.1.1 Política de seguridad en la relación con proveedores
15.1.2 Seguridad en el acuerdo con proveedores
15.1.3 Tecnología de la información y comunicacion en la cadena de suministro
15.2.1 Monitorización y revisión de la provisión de servicios

Fallos conocidos en versiones
12.6.1 Gestión de vulnerabilidades técnicas
12.6.2 Restricciones en la instalación de programas
14.2.4 Restricciones en cambios a paquetes de aplicaciones

Gestión de actualizaciones de seguridad ineficiente
12.5.1 Instalación de programas en sistemas en producción
14.2.2 Procedimiento de control de cambio en sistemas de información
14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación

Gestión ineficiente de contraseñas
9.2.3 Gestión de derechos de acceso privilegiado
9.2.4 Gestión de información secreta de autenticación

No existen registros de auditoría
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

Configuración de parámetros errónea.
14.1.1 Análisis y especificaciones de requisitos de seguridad de la información

Especificaciones para desarrolladores incompletas o confusas
9.4.5 Control de acceso a código fuente de programa
14.2.1 Política de desarrollo seguro
14.2.5 Principios para la ingeniería de sistemas seguros
14.2.6 Entorno seguro de desarrollo
14.2.7 Desarrollo externalizado

Fallos conocidos en versiones
12.6.1 Gestión de vulnerabilidades técnicas
14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación
14.2.4 Restricciones en cambios a paquetes de aplicaciones

Gestión de actualizaciones de seguridad ineficiente
12.5.1 Instalación de programas en sistemas en producción
12.6.1 Gestión de vulnerabilidades técnicas
12.6.2 Restricciones en la instalación de programas
14.2.2 Procedimiento de control de cambio en sistemas de información
14.2.3 Revisión técnica de las aplicaciones ante cambios en la plataforma de operación
14.2.4 Restricciones en cambios a paquetes de aplicaciones

No existen registros de auditoría	Pruebas de software insuficientes
12.4.1 Registro de eventos	14.2.8 Pruebas de seguridad del sistema
	14.2.9 Pruebas de aceptación del sistema
	14.3.1 Protección de la información de prueba

Violación de la legislación aplicable
10.1.1 Política en el uso de controles criptográficos
18.1.2 Derechos de propiedad intelectual

Acceso remoto no seguro
9.1.2 Acceso a redes y servicios de red
9.4.2 Procesos de inicio seguro de sesión
9.4.3 Sistema de gestión de contraseña
10.1.1 Política en el uso de controles criptográficos
10.1.2 Gestión de claves de criptografía

Asignación errónea de derechos de acceso	
9.2.2 Provisión de acceso a usuarios	
9.2.3 Gestión de derechos de acceso privilegiado	
9.2.5 Revisión de los derechos de acceso de usuarios	
9.2.6 Retirada o ajuste de los derechos de acceso	