Numeración	Control	Descripción	Global
5.1.1	Políticas para la seguridad de la información	Deben definirse, aprobarse por la dirección, publicarse y comunicarse a empleados y partes externas relevantes el conjunto de políticas para la seguridad de la información.	true
5.1.2	Revisión de las políticas para la seguridad de la información	Las politicas para la seguidad de la información deben revisarse a intervalos planificados o si existen cambios significativos para garantizar su eficacia, adecuación y conveniencia.	true
6.1.1	Roles y responsabilidades de la seguridad de la información	Se deben definir y asignar todas las responsabilidades sobre la seguridad de la información.	true
6.1.2	Segregación de tareas	Las responsabilidades y tareas que puedan entrar en conflicto deben segregarse para evitar oportunidades de modificación no autorizada o accidental o mal uso de los activos de la organización.	true
6.1.3	Contacto con las autoridades	Debe mantenerse contacto apropiado con autoridades relevantes.	true
6.1.4	Contacto con grupos de interés especial	Debe mantenerse contacto apropiado con grupos de interés especial u otros foros especializados en seguridad o asociaciones profesionales.	true
6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información debe aplicarse en la gestión de proyectos, sin importar el tipo de proyecto.	true
6.2.1	Política de dispositivos móviles	Debe adoptarse una política y medidas de apoyo a la seguridad para gestionar el riesgo introducido por el uso de dispositivos móviles con acceso a la información del negocio.	true
6.2.2	Teletrabajo	Se debe implementar una política para proteger la información accedida, procesada y almacenada en sitios de teletrabajo.	true
7.1.1	Selección	Los antecendentes laborales de los candidatos a puestos de trabajo debe ser verificados de acuerdo a la legislación vigente, de acuerdo al requisito de negocio, la clasificación de la información y el riesgo percibido.	true
7.1.2	Términos y condiciones del puesto de trabajo	Los contratos con el personal y los proveedores deben establecer sus responsabilidades y la de la organización sobre la seguridad de la información.	true
7.2.1	Responsabilidades de la dirección	La dirección debe requerir al personal y a contratistas que apliquen la seguridad de la información de acuerdo a las políticas y procedimientos establecidos en la organización.	true
Numeración	**Control**	**Descripción**	**Global**
7.2.2	Concienciación, educación y capacitación de la seguridad de la información	Todo el personal y contratistas cuando resulte relevante, deben recibir concienciación y formación, y actualizaciones periódicas sobre las politicas y procedimientos, en relación a la seguridad de la información.	true
7.2.3	Proceso disciplinario	Debe existir un proceso disciplinario formal y ser comunicado al pesonal, para ser aplicado en el caso de que provoquen una brecha en la seguridad de la información.	true

7.3.1	Finalización o cambios en las responsabilidades del puesto de trabajo	Las responsabilidades y deberes que se mantengan tras la terminación de la relación con empleados o contratistas deben estar definidas, comunicadas y procurar su cumplimiento.	true
8.1.1	Inventario de activos	Los activos asociados a la información y a las instalaciones de procesamiento de información deben estar identificados e incluidos en un inventario.	true
8.1.2	Propiedad de los activos	Los activos incluidos en el inventario deben tener un propietario.	true
8.1.3	Uso aceptable de los activos	Deben identificarse, documentarse e implementarse reglas para el uso aceptable de la información, los activos y las instalaciones de procesamiento.	true
8.1.4	Devolución de los activos	Todo el personal y partes externas que tengan en su poder activos de la organización, deben devolverlos ante la finalización de su empleo, contrato o acuerdo.	true
8.2.1	Clasificación de la información	La información debe ser clasificada en términos de requisitos legales, valor, criticidad y sensibilidad a modificación o revelación no autorizadas.	true
8.2.2	Etiquetado de la información	Debe desarrollarse e implementarse procedimientos apropiados para el etiquetado de información de acuerdo al esquema de clasificación de la información establecido en la organización.	true
8.2.3	Manejo de activos	Deben desarrollarse e implementarse procedimientos para el manejo de activos de acuerdo con el esquema de clasificación de la información establecido en la organización.	true
8.3.1	Gestión de medios removibles	Deben implementarse procedimientos para la gestión de los medios removibles de acuerdo al esquema de clasificación de la información establecido en la organización.	true
8.3.2	Desecho de medios	Los medios deben desecharse de manera segura cuando ya no tengan uso, mediante procedimientos formales.	true
8.3.3	Tránsito de medios físicos	Los medios que contengan información deben protegerse de accesos no autorizados, usos indebidos o daño durante el transporte.	true
Numeración	**Control**	**Descripción**	**Global**
9.1.1	Política de control de acceso	La organización debe establecer, documentar y revisar en base a los requisitos del negocio y de la seguridad de la información, una política de control de acceso.	true
9.1.2	Acceso a redes y servicios de red	El acceso a las redes y a los servicios de red deben otorgarse unicamete a los usuarios específicamente autorizados a utilizarlos.	true
9.2.1	Alta y baja de usuario	Debe implementarse un proceso formal de alta y baja de usuarios que permita la asignación de derechos de acceso a la información.	true
9.2.2	Provisión de acceso a usuarios	Debe implementarse un proceso formal de provisión para otorgar o retirar derechos de accesos a todos los tipos de usuarios sobre todos los sistemas de información.	true
9.2.3	Gestión de derechos de acceso privilegiado	Debe controlarse y restringirse la entrega y uso de derechos de acceso privilegiados.	true

9.2.4	Gestión de información secreta de autenticación	La ubicación de la información secreta de autenticación de los usuarios debe controlarse mediante un proceso formal de gestión.	true
9.2.5	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar periódicamente los derechos de acceso de los usuarios.	true
9.2.6	Retirada o ajuste de los derechos de acceso	Los derechos de acceso a la información y a las instalaciones de procesamiento de información de empleados y partes externas deben ser retirados ante la finalización de la relación o modificados ante cambios de la misma.	true
9.3.1	Uso de información secreta de autenticación	El personal debe tener la responsabilidad de cumplir las prácticas definidas por la organización para el uso de la información secreta de autenticación.	true
9.4.1	Restricción del acceso a la información	El acceso a la información y a las funciones de los sistemas de información debe estar restringido de acuerdo a la política de control de acceso.	true
9.4.2	Procesos de inicio seguro de sesión	Cuando sea requerido por la política de control de acceso, el acceso a los sistemas de información y aplicaciones deben estar controlados por procedimientos de inicio de sesión seguros.	true
9.4.3	Sistema de gestión de contraseña	El sistema de gestión de contraseña debe ser interactivo y garantizar la calidad de las mismas.	true
9.4.4	Uso de programas privilegiados de utilidad	El uso de aplicaciones utilitarias que puedan anular control de seguridad de los sistemas debe estar restringido y firmemente controlado.	true
9.4.5	Control de acceso a código fuente de programa	El acceso a código fuente debe estar restringido.	true
10.1.1	Política en el uso de controles criptográficos	Debe desarrollarse e implementarse una política sobre el uso de controles criptográficos para proteger la información.	true
Numeración	**Control**	**Descripción**	**Global**
10.1.2	Gestión de claves de criptografía	Una política sobre el uso, protección y duración de las llaves criptográficas deben desarrollarse e implementarse durante todo su ciclo de vida.	true
11.1.1	Perímetro de seguridad física	Deben definirse y utilizarse perímetros de seguridad para la protección de áreas que contengan información crítica o sensible e instalaciones de procesamiento de información.	true
11.1.2	Controles de acceso físico	Las áreas seguras deben protegerse por controles de entrada adecuados que otorguen acceso solo al personal autorizado.	true
11.1.3	Seguridad de oficinas, salas e instalaciones	Debe diseñarse y aplicarse seguridad física para oficinas, salas e instalaciones.	true
11.1.4	Protección contra amenazas externas y ambientales	Debe diseñarse y aplicarse seguridad para la protección física contra desastres naturales, ataques maliciosos o accidentes.	true
11.1.5	Trabajo en áreas seguras	Deben diseñarse y aplicarse procedimentos para el trabajo en áreas seguras.	true
11.1.6	Áreas de entrega y carga	Los puntos de acceso para entrega y carga de material, como cualquier otro punto vulnerable al acceso no autorizado debe ser controlado, y de ser posible aislado de las areas de procesamiento de información.	true

11.2.1	Ubicación y protección de equipos	Los equipos deben ubicarse y protegerse para reducir el riesgo de amenazas ambientales y de accesos no autorizados.	true
11.2.2	Servicios de suministro	Los equipos deben estar protegidos contra fallas de alimentación electrica y otros fallos de suministro.	true
11.2.3	Seguridad del cableado	El cableado de potencia que alimente los sistemas y de comunicaciones que transporte información debe protegerse de intercepciones, interferencias o daños.	true
11.2.4	Mantenimiento de equipos	Los equipos deben ser correctamente mantenidos para garantizar su disponibilidad e integridad.	true
11.2.5	Retirada de activos	El equipamiento, aplicaciones e información no deben llevarse fuera de las instalaciones seguras sin la debida autorización.	true
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Debe aplicarse la seguridad sobre equipos fuera de las instalaciones considerando los diferentes riesgos del trabajo fuera de las instalaciones de la organización.	true
11.2.7	Seguridad en el desecho o reutilización de equipos	Los elementos de equipamiento que contengan medios de almacenamiento de información deben ser verificados para asegurar la eliminación o sobreescritura de información sensible, licencias antes de su desecho o reuso.	true
11.2.8	Equipos de usuario desatendido	Los usuarios deben asegurar que sus equipos tengan apropiada protección cuando queden desatendidos.	true
Numeración	**Control**	**Descripción**	**Global**
11.2.9	Política de pantalla y escritorio despejado	Una política de escritorio despejado de papeles y medio removibles y de pantalla de equipos de procesamiento limpia debe definirse y adoptarse.	true
12.1.1	Procedimientos operativos documentados	Los procedimientos de operación deben estar documentados y puestos a disposición de los usuarios que los necesiten.	true
12.1.2	Gestión del cambio	Deben controlarse los cambios en la organización, en los procesos de negocio, en las instalaciones de procesamiento y sistemas, cuando afecten a la seguridad de la información.	true
12.1.3	Gestión de la capacidad	Debe monitorizarse, ajustarse y proyectarse los requisitos futuros de capacidad del uso de los recursos para garantizar su correcto desempeño.	true
12.1.4	Separación de entornos de desarrollo, prueba y operación	Los entornos de desarrollo, prueba y operación deben estar separado para reducir el riesgo de accesos no autorizados o cambios sobre el entorno de operaciones.	true
12.2.1	Controles contra código malicioso	Deben implementarse controles de detección, prevención y recuperación contra codigo maliciso, combinados con la debida concienciación de los usuarios.	true
12.3.1	Copia de seguridad de la información	Copias de seguridad de la información, los sistemas, imágenes deben realizarse y probadas de forma regular de acuerdo a la política de copia de seguridad de la organización.	true
12.4.1	Registro de eventos	Deben producirse, mantenerse y revisarse periodicamente los registros de la actividad de los usuarios, los fallos en los sistemas y los eventos de seguridad.	true

12.4.2	Protección de la información del registro de eventos	Las instalaciones de registro y la información de registros deben protegerse contra manipulación y accesos no autorizados.	true
12.4.3	Registro de administrador y operador	La actividad de los adminstradores y operadores de sistemas debe registrarse, protegiendo estos registros y revisándolos periódicamente.	true
12.4.4	Sincronización de reloj	Los rejoles de todos los sistemas de procesamiento de información relevantes, ya sea de la organizacion o del dominio de seguridad, deben sincronizarse respecto de una única fuente.	true
12.5.1	Instalación de programas en sistemas en producción	Deben implementarse procedimientos para controlar la instalación de aplicaciones en sistemas en operación.	true
12.6.1	Gestión de vulnerabilidades técnicas	La información sobre vulnerabilidades técnicas sobre los sistemas de la organización debe ser obtenida tan pronto como esté disponible de manera de evaluar la exposición y aplicar medidas apropiadas para reducir riesgos.	true
12.6.2	Restricciones en la instalación de programas	Deben establecerse e implementarse reglas que controlen la instalación de aplicaciones por parte de los usuarios.	true
Numeración	**Control**	**Descripción**	**Global**
12.7.1	Controles de la auditoría de sistemas de información	Los requisitos y actividades de auditoría que involucren la verificación de sistemas en producción deben planificarse cuidadosamente y estar acordados para reducir interrupciones sobre los procesos de negocio.	true
13.1.1	Controles de red	Las redes deben gestionarse y controlarse para proteger la información de sistemas y aplicaciones.	true
13.1.2	Seguridad de servicios de red	Los requisitos gestión, nivel de servicio y mecanismos de seguridad sobre todos los servicios de red deben estar identificados y ser incluidos tanto sean servicios internos o externos.	true
13.1.3	Segregación de redes	Deben segregarse los grupos de servicios de información, sistemas de información y usuarios en redes.	true
13.2.1	Políticas y procedimientos para el intercambio de información	Deben aplicarse políticas, procedimientos y controles formales para proteger la transferencia de información a través de cualquier tipo de medio de comunicación.	true
13.2.2	Acuerdos de intercambio de información	Deben definirse acuerdos que atiendan la seguridad sobre la transferencia de información del negocio entre la organización y las partes externas.	true
13.2.3	Mensajería electrónica	La información incluida en mensajería electrónica debe ser protegida de forma apropiada.	true
13.2.4	Acuerdos de confidencialidad y no divulgación	Debe identificarse, revisarse regularmente y documentarse los requisitos de confidencialidad y no divulgación de la organización sobre la protección de la información del negocio.	true
14.1.1	Análisis y especificaciones de requisitos de seguridad de la información	Los requisitos relacionados con la seguridad de la información debe incluirse para los nuevos sistemas de información o para la mejora de sistemas existentes.	true

14.1.2	Seguridad del servicio de aplicacion en redes públicas	La información trasmitida por aplicaciones o servicios a trvés de redes públicas debe ser protegida de actividades fraudulentas, disputas contractuales y modificacion o divulgación no autorizada.	true
14.1.3	Protección de transacciones en servicio de aplicación	La información involucrada en transacciones de servicios debe ser protegida para evitar transmisiones incompletas, ruteo erróneo así como alteración, revelación, duplicación y repetición no autorizadas.	true
14.2.1	Política de desarrollo seguro	Deben establecerse y aplicarse reglas al desarrollo de sistemas de información en la organización.	true
14.2.2	Procedimiento de control de cambio en sistemas de información	Los cambios sobre los sistemas de información durante su ciclo de vida deben estar controlados mediante procedimientos formales de control de cambio.	true
Numeración	**Control**	**Descripción**	**Global**
14.2.3	Revisión técnica de las aplicaciones ante cambios en la plataforma de operación	Cuando las plataformas operativas sufran cambios, las aplicaciones críticas de negocio deben ser revisadas y probadas para garantizar que no exsiten impactos adversos sobre la operación o la seguridad de la información.	true
14.2.4	Restricciones en cambios a paquetes de aplicaciones	La modificación de paquetes de aplicaciones debe restringirse y limitarse unicamente a cambios necesarios y estos deben ser controlados de forma estricta.	true
14.2.5	Principios para la ingeniería de sistemas seguros	Deben establecerse principios para la ingeniería de sistemas seguros, que sean documentados, mantenidos y aplicados a los esfuerzos de la organización para la implementación de cualquier sistema de información.	true
14.2.6	Entorno seguro de desarrollo	La organización debe establecer y proteger los entornos seguros de desarrollo que cubran todo el ciclo de vida.	true
14.2.7	Desarrollo externalizado	La organización debe supervisar y monitorizar las actividades de los proveedores de los desarrollos externalizados.	true
14.2.8	Pruebas de seguridad del sistema	Las pruebas de seguridad funcional de las aplicaciones deben ser llevadas adelante durante el período de desarrollo.	true
14.2.9	Pruebas de aceptación del sistema	Deben definirse y establecerse programas de pruebas y criterios de aceptación para nuevos sistemas de información, nuevas versiones y actualizaciones.	true
14.3.1	Protección de la información de prueba	Los datos de prueba deben ser seleccionados, cuidadosamente, estar protegidos y controlados.	true
15.1.1	Política de seguridad en la relación con proveedores	Los requisitos de seguridad de la información para reducir riesgos asociados con el acceso de proveedores a los activos de la organización, deben acordarse y documentarse.	true
15.1.2	Seguridad en el acuerdo con proveedores	Todos los requisitos de seguridad de la información relevantes deben definirse y acordarse con cada proveedor que pueda acceder, procesar, almacenar, comunicar información y proveer infraestructuras IT.	true

15.1.3	Tecnología de la información y comunicacion en la cadena de suministro	Los acuerdos con proveedores deben incluir requisitos que reduzcan los riesgos asociados a la información, tecnologías de la comunicación y cadena de suministros.	true
15.2.1	Monitorización y revisión de la provisión de servicios	La organización debe monitorizar, revisar y auditar la provisión de servicios regularmente.	true
15.2.2	Gestión de cambios en la provisión de servicios	Los cambios en la provisión de servicio, incluyendo el mantenimiento y mejoras de las politicas, procedimentos y procesos de seguridad de la información exstentes, deben gestionarse considerando la evaluación de riesgos.	true
Numeración	**Control**	**Descripción**	**Global**
16.1.1	Responsabilidades y procedimientos	Deben establecerse las responsabilidades de la dirección y sobre los procedimientos para garantizar una respuesta rápida, eficaz y ordenada ante incidencias de seguridad de la información.	true
16.1.2	Reporte de eventos sobre la seguridad de la información	Los incidentes de seguridad de la información deben ser reportados tan pronto como sea posible a través de canales de comunicación debidamente gestionados.	true
16.1.3	Reporte de debilidades en la seguridad de la información	El personal y los contratistas que utilicen los sistemas de información y los servicios de la organización deben ser responsables de notificar cualquier debilidad en la seguridad que observen o de la que sospechen.	true
16.1.4	Valoración y decisión sobre los eventos de seguridad de la información	Los eventos en la seguridad de la información deben ser evaluados para determinar si serán clasificados como incidencias de seguridad de la información para ser gestionados de forma adecuada.	true
16.1.5	Respuesta a los incidentes de seguridad de la información	Las incidencias de seguridad de la información deben tener una respuesta acorde a los procedimientos documentados a tal fin.	true
16.1.6	Aprendizaje de los incidentes de seguridad de la información	El conocimiento obtenido de análisis y la resolución de los incidentes de seguridad de la información debe ser utilizado para procurar reducir la probabilidad y el impacto de incidencias futuras.	true
16.1.7	Recolección de evidencias	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de la información que pueda servir de evidencia.	true
17.1.1	Planificacion de la continuidad de la seguridad de la información	La organización debe definir los requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información ante situaciones adversas.	true
17.1.2	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener los procesos y procedimientos para garantizar el nivel requerido de continuidad de seguridad de la información durante situaciones adversas.	true
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar la continuidad de la seguridad de la información establecida e implementada a través de los controles en intervalos regulares para garantizar su validez y efectividad.	true

17.2.1	Disponibilidad de las instalaciones de procesamiento de información	Las instalaciones de procesamiento de información deben contar con la redundancia suficiente para contar con sus requisitos de disponibilidad.	true
Numeración	**Control**	**Descripción**	**Global**
18.1.1	Identificación de legislación aplicable y requisitos contractuales	Deben identificarse de forma explícita, documentarse y mantenerse actualizados todos los requisitos legales, regulatorios, contractuales relevantes para cada sistemas de información y la operación de la organización.	true
18.1.2	Derechos de propiedad intelectual	Deben implementarse procedimientos apropiados para asegurar el cumplimiento de requisitos legales, regulatorios y contractuales relacionados con los derechos de propiedad intelectual y el uso de sistemas de información.	true
18.1.3	Protección de registros	Los registros deben protegerse de pérdida, destrucción, falsificación y acceso no autorizado de acuerdo a requisitos legales, regulatorios, contractuales y de negocio.	true
18.1.4	Privacidad y protección de información de identificación personal	La protección de la privacidad de la información de identificación personal debe aplicarse de acuerdo a la legislación aplicable.	true
18.1.5	Regulación de controles de criptografía	Los controles criptográficos deben utilizarse de acuerdo a los acuerdos, legislación y regulaciones relevantes.	true
18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización con la seguridad de la información (objetivos de control, controles, políticas, procedimientos y procesos) deben revisarse de manera independiente en períodos planificados o ante cambios.	true
18.2.2	Cumplimiento de politicas y normas de seguridad	Los responsables de áreas de negocio deben identificar como revisar el cumplimiento del procesamiento de la información y procedimientos de seguridad, de acuerdo a politicas, estándares y requisitos de seguridad.	true
18.2.3	Revisión de cumplimiento técnico	Los sistemas de información deben ser revisados periodicamente para garantizar el cumplimiento de las políticas y estándares de seguridad de la información.	true