Controles ISO IEC 27002

CAPÍTULOS DE CONTROLES DE SEGURIDAD

- 5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
- 6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
- 7. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS
- 8. GESTIÓN DE ACTIVOS
- 9. CONTROL DE ACCESO
- 10. CRIPTOGRAFÍA
- 11. SEGURIDAD FÍSICA Y DEL ENTORNO
- 12. SEGURIDAD DE LAS OPERACIONES
- 13. SEGURIDAD DEL AS COMUNICACIONES
- 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN
- 15. RELACIÓN CON PROVEEDORES
- 16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
- 17. ASPECTOS DE SEGURIDAD DE INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
- 18. CUMPLIMIENTO

5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

5.1 DIRECTRICES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Objetivo: Proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes.

5.1.1 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

Un conjunto de políticas para la seguridad de la información debería ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes .

5.1.2 REVISIÓN DE LAS POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad de la información deberían revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1 ORGANIZACIÓN INTERNA

Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.

6.1.1 ROLES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN

Todas las responsabilidades en seguridad de la información deberían definirse y asignarse.

6.1.2 SEGREGACIÓN DE TAREAS

Las funciones y áreas de responsabilidad deberían segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.

6.1.3 CONTACTO CON LAS AUTORIDADES

Deberían mantenerse los contactos apropiados con las autoridades pertinentes.

6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL

Deberían mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.

6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS

La seguridad de la información debería tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.

6.2 LOS DISPOSITIVOS MÓVILES Y EL TELETRABAJO

Objetivo: Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles.

6.2.1 POLÍTICA DE DISPOSITIVOS MÓVILES

Se debería adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.

6.2.2 TELETRABAJO

Se debería implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.

7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS

7.1 ANTES DEL EMPLEO

Objetivo: Para asegurarse que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.

7.1.1 INVESTIGACIÓN DE ANTECEDENTES

La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debería llevar a cabo de acuerdo con las leyes, normativa y códigos éticos que sean de aplicación y debería ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.

7.1.2 TÉRMINOS Y CONDICIONES DEL EMPLEO

Cómo parte de sus obligaciones contractuales, los empleados y contratistas deberían establecer los términos y condiciones en su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.

7.2 DURANTE EL EMPLEO

Objetivo: Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información.

7.2.1 RESPONSABILIDADES DE GESTIÓN

La dirección debería exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.

7.2.2 CONCIENCIACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Todos los empleados de la organización y, cuando corresponda, los contratistas, deberían recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.

7.2.3 PROCESO DISCIPLINARIO

Debería existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.

7.3 FINALIZACIÓN DEL EMPLEO O CAMBIO EN EL PUESTO DE TRABAJO

Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo.

7.3.1 RESPONSABILIDADES ANTE LA FINALIZACIÓN O CAMBIO

Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deberían definir, comunicar al empleado o contratista y se deberían cumplir.

8 GESTIÓN DE ACTIVOS

8.1 RESPONSABILIDAD SOBRE LOS ACTIVOS

Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.

8.1.1 INVENTARIO DE ACTIVOS

La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deberían estar claramente identificados y debería elaborarse y mantenerse un inventario.

8.1.2 PROPIEDAD DE LOS ACTIVOS

Todos los activos que figuran en el inventario deberían tener un propietario.

8.1.3 USO ACEPTABLE DE LOS ACTIVOS

Se deberían identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.

8.1.4 DEVOLUCIÓN DE ACTIVOS

Todos los empleados y terceras partes deberían devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.

8.2 CLASIFICACIÓN DE LA INFORMACIÓN

Objetivo: Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.

8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN

La información debería ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.

8.2.2 ETIQUETADO DE LA INFORMACIÓN

Debería desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.

8.2.3 MANIPULADO DE LA INFORMACIÓN

Debería desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.

8.3 MANIPULACIÓN DE LOS SOPORTES

Objetivo: Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en soportes.

8.3.1 GESTIÓN DE SOPORTES EXTRAÍBLES

Se deberían implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.

8.3.2 ELIMINACIÓN DE SOPORTES

Los soportes deberían eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.

8.3.3 SOPORTES FÍSICOS EN TRÁNSITO

Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deberían estar protegidos contra accesos no autorizados, usos indebidos o deterioro.

9 CONTROL DE ACCESO

9.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO

OBJETIVO: Limitar el acceso a los recursos de tratamiento de información y a la información.

9.1.1 POLÍTICA DE CONTROL DE ACCESO

Se debería establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.

9.1.2 ACCESO A LAS REDES Y A LOS SERVICIOS DE RED

Únicamente se debería proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.

9.2 GESTIÓN DE ACCESO DE USUARIO

OBJETIVO: Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.

9.2.1 REGISTRO Y BAJA DE USUARIO

Debería implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.

9.2.2 PROVISIÓN DE ACCESO DE USUARIO

Debería implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.

9.2.3 GESTIÓN DE PRIVILEGIOS DE ACCESO

La asignación y el uso de privilegios de acceso debería estar restringida y controlada.

9.3 RESPONSABILIDADES DEL USUARIO

OBJETIVO: Para que los usuarios se hagan responsables de salvaguardar su información de autenticación.

9.3.1 USO DE LA INFORMACIÓN SECRETA DE AUTENTICACIÓN

Se debería requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.

9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

OBJETIVO: Prevenir el acceso no autorizado a los sistemas y aplicaciones.

9.4.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN

Se debería restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.

9.4.2 PROCEDIMIENTOS SEGUROS DE INICIO DE SESIÓN

Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debería controlar por medio de un procedimiento seguro de inicio de sesión.

9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS

Los sistemas para la gestión de contraseñas deberían ser interactivos y establecer contraseñas seguras y robustas.

9.4.4 USO DE UTILIDADES CON PRIVILEGIOS DEL SISTEMA

Se debería restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.

9.4.5 CONTROL DE ACCESO AL CÓDIGO FUENTE DE LOS PROGRAMAS

Se debería restringir el acceso al código fuente de los programas.

10 CRIPTOGRAFÍA

10.1 CONTROLES CRIPTOGRÁFICOS

OBJETIVO: Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

10.1.1 POLÍTICA DE USO DE LOS CONTROLES CRIPTOGRÁFICOS

Se debería desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.

10.1.2 GESTIÓN DE CLAVES

Se debería desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.

11 SEGURIDAD FÍSICA Y DEL ENTORNO

11.1 ÁREAS SEGURAS

OBJETIVO: Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.

11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA

Se deberían utilizar perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.

11.1.2 CONTROLES FÍSICOS DE ENTRADA

Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.

11.1.3 SEGURIDAD DE OFICINAS, DESPACHOS Y RECURSOS

Para las oficinas, despachos y recursos, se debería diseñar y aplicar la seguridad física.

11.1.4 PROTECCIÓN CONTRA LAS AMENAZAS EXTERNAS Y AMBIENTALES

Se debería diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.

11.1.5 EL TRABAJO EN ÁREAS SEGURAS

Se deberían diseñar e implementar procedimientos para trabajar en las áreas seguras.

11.1.6 ÁREAS DE CARGA Y DESCARGA

Deberían controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.

11.2 SEGURIDAD DE LOS EQUIPOS

OBJETIVO: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.

11.2.1 EMPLAZAMIENTO Y PROTECCIÓN DE EQUIPOS

Los equipos deberían situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales, así como las oportunidades de que se produzcan accesos no autorizados.

11.2.2 INSTALACIONES DE SUMINISTRO

Los equipos deberían estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.

11.2.3 SEGURIDAD DEL CABLEADO

El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debería estar protegido frente a interceptaciones, interferencias o daños.

11.2.4 MANTENIMIENTO DE LOS EQUIPOS

Los equipos deberían recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.

11.2.5 RETIRADA DE MATERIALES PROPIEDAD DE LA EMPRESA

Sin autorización previa, los equipos, la información o el software no deberían sacarse de las instalaciones.

11.2.6 SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES

Deberían aplicarse medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.

11.2.7 REUTILIZACIÓN O ELIMINACIÓN SEGURA DE EQUIPOS

Todos los soportes de almacenamiento deberían ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.

11.2.8 EQUIPO DE USUARIO DESATENDIDO

Los usuarios deberían asegurarse DE QUE el equipo desatendido tiene la protección adecuada.

11.2.9 POLÍTICA DE PUESTO DE TRABAJO DESPEJADO Y PANTALLA LIMPIA

Debería adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.

12 SEGURIDAD DE LAS OPERACIONES

12.1 PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES

OBJETIVO: Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.

12.1.1 DOCUMENTACIÓN DE PROCEDIMIENTOS DE LOS OPERACIÓN

Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de información deberían ser controlados.

12.1.2 GESTIÓN DE CAMBIOS

Deberían documentarse y mantenerse procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.

12.1.3 GESTIÓN DE CAPACIDADES

Se debería supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.

12.1.4 SEPARACIÓN DE LOS RECURSOS DE DESARROLLO, PRUEBA Y OPERACIÓN

Deberían separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.

12.2 PROTECCIÓN CONTRA EL SOFTWARE MALICIOSO (MALWARE)

OBJETIVO: Asegurar que los recursos de tratamiento de información y la información están protegidos contra el malware.

12.2.1 CONTROLES CONTRA EL CÓDIGO MALICIOSO

Se deberían implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.

12.3 COPIAS DE SEGURIDAD

OBJETIVO: Se deberían realizar copias de seguridad de la información, del software y del sistema y se deberían verificar periódicamente, de acuerdo a la política de copias de seguridad acordada.

12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACIÓN

Se deberían realizar copias de seguridad de la información, del software y del sistema y se deberían verificar periódicamente de acuerdo a la política de copias de seguridad acordada.

12.4 REGISTROS Y SUPERVISIÓN

OBJETIVO: Registrar eventos y generar evidencias.

12.4.1 REGISTRO DE EVENTOS

Se deberían registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.

12.4.2 PROTECCIÓN DE LA INFORMACIÓN DEL REGISTRO

Los dispositivos de registro y la información del registro deberían estar protegidos contra manipulaciones indebidas y accesos no autorizados.

12.4.3 REGISTROS DE ADMINISTRACIÓN Y OPERACIÓN

Se deberían registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.

12.4.4 SINCRONIZACIÓN DEL RELOJ

Los relojes de todos los sistemas de tratamiento de información dentro de una organización o de un dominio de seguridad, deberían estar sincronizados con una única fuente de tiempo precisa y acordada.

12.5 CONTROL DEL SOFTWARE EN EXPLOTACIÓN

OBJETIVO: Asegurar la integridad del software en explotación.

12.5.1 INSTALACIÓN DEL SOFTWARE EN EXPLOTACIÓN

Se deberían implementar procedimientos para controlar la instalación del software en explotación.

12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA

OBJETIVO: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.

12.6.1 GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS

Se debería obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.

12.6.2 RESTRICCIÓN EN LA INSTALACIÓN DE SOFTWARE

Se deberían establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.

12.7 CONSIDERACIONES SOBRE LA AUDITORIA DE SISTEMAS DE INFORMACIÓN

OBJETIVO: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.

12.7.1 CONTROLES DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN

Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deberían ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.

13 SEGURIDAD DE LAS COMUNICACIONES

13.1 GESTIÓN DE LA SEGURIDAD DE REDES

Objetivo: Asegurar la protección de la información en las redes y los recursos de tratamiento de la información.

13.1.1 CONTROLES DE RED

Las redes deberían ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.

13.1.2 SEGURIDAD DE LOS SERVICIOS DE RED

Se deberían identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deberían incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.

13.1.3 SEGREGACIÓN EN REDES

Los grupos de servicios de información, los usuarios y los sistemas de información deberían estar segregados en redes distintas.

13.2 INTERCAMBIO DE INFORMACIÓN

Objetivo: Mantener la seguridad en la información que se transfiere dentro de una organización y con cualquier entidad externa.

13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACIÓN

Deberían establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.

13.2.2 ACUERDOS DE INTERCAMBIO DE INFORMACIÓN

Deberían establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.

13.2.3 MENSAJERÍA ELECTRÓNICA

La información que sea objeto de mensajería electrónica debería estar adecuadamente protegida.

13.2.4 ACUERDOS DE CONFIDENCIALIDAD O NO REVELACIÓN

Deberían identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación.

14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

14.1 REQUISITOS DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

Objetivo: Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.

14.1.1 ANÁLISIS DE REQUISITOS Y ESPECIFICACIONES DE SEGURIDAD DE LA INFORMACIÓN

Los requisitos relacionados con la seguridad de la información deberían incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.

14.1.2 ASEGURAR LOS SERVICIOS DE APLICACIONES EN REDES PÚBLICAS

La información involucrada en aplicaciones que pasan a través de redes públicas debería ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas.

14.1.3 PROTECCIÓN DE LAS TRANSACCIONES DE SERVICIOS DE APLICACIONES

La información involucrada en las transacciones de servicios de aplicaciones debería ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autorizadas.

14.2 SEGURIDAD EN EL DESARROLLO Y EN LOS PROCESOS DE SOPORTE

Objetivo: Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de los sistemas de información.

14.2.1 POLÍTICA DE DESARROLLO SEGURO

Se deberían establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.

14.2.2 PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS

La implantación de cambios a lo largo del ciclo de vida del desarrollo debería controlarse mediante el uso de procedimientos formales de control de cambios.

14.2.3 REVISIÓN TÉCNICA DE LAS APLICACIONES TRAS EFECTUAR CAMBIOS EN EL SISTEMA OPERATIVO

Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deberían ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización.

14.2.4 RESTRICCIONES A LOS CAMBIOS EN LOS PAQUETES DE SOFTWARE

Se deberían desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deberían ser objeto de un control riguroso.

14.2.5 PRINCIPIOS DE INGENIERÍA DE SISTEMAS SEGUROS

Principios de ingeniería de sistemas seguros se deberían establecer, documentar, mantener y aplicarse a todos los esfuerzos de implantación de sistemas de información.

14.2.6 ENTORNO DE DESARROLLO SEGURO

Las organizaciones deberían establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.

14.2.7 EXTERNALIZACIÓN DEL DESARROLLO DE SOFTWARE

El desarrollo de software externalizado debería ser supervisado y controlado por la organización.

14.2.8 PRUEBAS FUNCIONALES DE SEGURIDAD DE SISTEMAS

Se deberían llevar a cabo pruebas de la seguridad funcional durante el desarrollo.

14.2.9 PRUEBAS DE ACEPTACIÓN DE SISTEMAS

Se deberían establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.

14.3 DATOS DE PRUEBA

Objetivo: Asegurar la protección de los datos de prueba.

14.3.1 PROTECCIÓN DE LOS DATOS DE PRUEBA

Los datos de prueba se deberían seleccionar con cuidado y deberían ser protegidos y controlados.

15 RELACIÓN CON PROVEEDORES

15.1 SEGURIDAD EN LAS RELACIONES CON PROVEEDORES

Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

15.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES

Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deberían acordarse con el proveedor y quedar documentados.

15.1.2 REQUISITOS DE SEGURIDAD EN CONTRATOS CON TERCEROS

Todos los requisitos relacionados con la seguridad de la información deberían establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura "Tecnología de la Información".

15.1.3 CADENA DE SUMINISTRO DE TECNOLOGÍA DE LA INFORMACIÓN Y DE LAS COMUNICACIONES

Los acuerdos con proveedores deberían incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.

15.2 GESTIÓN DE LA PROVISIÓN DE SERVICIOS DEL PROVEEDOR

Objetivo: Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores.

15.2.1 CONTROL Y REVISIÓN DE LA PROVISIÓN DE SERVICIOS DEL PROVEEDOR

Las organizaciones deberían controlar, revisar y auditar regularmente la provisión de servicios del proveedor.

15.2.2 GESTIÓN DE CAMBIOS EN LA PROVISIÓN DEL SERVICIO DEL PROVEEDOR

Se deberían gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados, así como la reapreciación de los riesgos.

16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

16.1 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.

16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS

Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.

16.1.2 NOTIFICACIÓN DE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

Los eventos de seguridad de la información se deberían notificar por los canales de gestión adecuados lo antes posible.

16.1.3 NOTIFICACIÓN DE PUNTOS DÉBILES DE LA SEGURIDAD

Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deberían ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.

16.1.4 EVALUACIÓN Y DECISIÓN SOBRE LOS EVENTOS DE SEGURIDAD DE INFORMACIÓN

Los eventos de seguridad de la información deberían ser evaluados y debería decidirse si se clasifican como incidentes de seguridad de la información.

16.1.5 RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Los incidentes de seguridad de la información deberían ser respondidos de acuerdo con los procedimientos documentados.

16.1.6 APRENDIZAJE DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de información debería utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.

16.1.7 RECOPILACIÓN DE EVIDENCIAS

La organización debería definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de información que puede servir de evidencia.

17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

17.1 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

Objetivo: La continuidad de la seguridad de la información debería formar parte de los sistemas de gestión de la continuidad de negocio de la organización.

17.1.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

La organización debería determinar sus necesidades de seguridad de la información y de continuidad para la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

17.1.2 IMPLEMENTAR LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.

17.1.3 VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

La organización debería comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.

17.2 REDUNDANCIAS

Objetivo: Asegurar la disponibilidad de los recursos de tratamiento de la información.

17.2.1 DISPONIBILIDAD DE LOS RECURSOS DE TRATAMIENTO DE LA INFORMACIÓN

Los recursos de tratamiento de la información deberían ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.

18 CUMPLIMIENTO

18.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES

Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.

18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES

Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deberían definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización.

18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL (DPI)

Deberían implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

18.1.3 PROTECCIÓN DE LOS REGISTROS DE LA ORGANIZACIÓN

Los registros deberían estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.

18.1.4 PROTECCIÓN Y PRIVACIDAD DE LA INFORMACIÓN DE CARÁCTER PERSONAL

Debería garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.

18.1.5 REGULACIÓN DE LOS CONTROLES CRIPTOGRÁFICOS

Los controles criptográficos se deberían utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.

18.2 REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN

Objetivo: Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.

18.2.1 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN

El enfoque de la organización para la gestión de la seguridad de la información y su implantación, es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información, debería someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.

18.2.2 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD

Los directivos deberían asegurarse que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable.

18.2.3 COMPROBACIÓN DEL CUMPLIMIENTO TÉCNICO

Debería comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.