**Controles ISO 27002**

Tabla de contenido

[A5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 1](#_Toc81624576)

[5.1.1 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN 1](#_Toc81624577)

[5.1.2 REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 2](#_Toc81624578)

[***ALGUNOS CONSEJOS PRÁCTICOS*** 3](#_Toc81624579)

[A6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 3](#_Toc81624580)

[6.1 ORGANIZACIÓN INTERNA 4](#_Toc81624581)

[**6.1.1 FUNCIONES Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN** 4](#_Toc81624582)

[**6.1.2 SEGREGACIÓN DE TAREAS** 4](#_Toc81624583)

[**6.1.3 CONTACTO CON AUTORIDADES** 6](#_Toc81624584)

[**6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL.** 7](#_Toc81624585)

[**6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.** 7](#_Toc81624586)

[6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO 9](#_Toc81624587)

[**6.2.1 POLÍTICA DE DISPOSITIVOS MÓVILES** 9](#_Toc81624588)

[**6.2.2 TELETRABAJO** 11](#_Toc81624589)

[A7 SEGURIDAD RELATIVA A LOS RECURSOS 13](#_Toc81624590)

[7.1 PREVIO AL EMPLEO 14](#_Toc81624591)

[**7.1.1 SELECCIÓN** 15](#_Toc81624592)

[**7.1.2 TÉRMINOS Y CONDICIONES DE EMPLEO** 16](#_Toc81624593)

[7.2 DURANTE EL EMPLEO 17](#_Toc81624594)

[**7.2.1 RESPONSABILIDADES DE LA DIRECCIÓN** 17](#_Toc81624595)

[**7.2.2 CONCIENTIZACIÓN, EDUCACIÓN Y FORMACIÓN EN SEGURIDAD DE LA INFORMACIÓN** 18](#_Toc81624596)

[**7.2.3 PROCESO DISCIPLINARIO** 19](#_Toc81624597)

[7.3 FINALIZACIÓN O CAMBIO DE LA RELACIÓN LABORAL O EMPLEO 19](#_Toc81624598)

[**7.3.1 RESPONSABILIDADES EN LA DESVINCULACIÓN** 20](#_Toc81624599)

[A8 GESTION DE ACTIVOS 20](#_Toc81624600)

[8.1 RESPONSABILIDAD DE LOS ACTIVOS 21](#_Toc81624601)

[**8.1.1 INVENTARIO DE ACTIVOS** 22](#_Toc81624602)

[**8.1.2 PROPIEDAD DE LOS ACTIVOS** 22](#_Toc81624603)

[**8.1.3 USO ACEPTABLE DE LOS ACTIVOS** 23](#_Toc81624604)

[**8.1.4 DEVOLUCIÓN DE ACTIVOS** 23](#_Toc81624605)

[8.2 CLASIFICACIÓN DE LA INFORMACIÓN 24](#_Toc81624606)

[**8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN** 24](#_Toc81624607)

[**8.2.2 ETIQUETADO DE LA INFORMACIÓN** 25](#_Toc81624608)

[**8.2.3 MANEJO DE LOS ACTIVOS** 26](#_Toc81624609)

[8.3 MANIPULACIÓN DE SOPORTES 27](#_Toc81624610)

[**8.3.1 GESTIÓN DE SOPORTES EXTRAÍBLES** 27](#_Toc81624611)

[**8.3.2 ELIMINACIÓN DE SOPORTES** 28](#_Toc81624612)

[**8.3.3 TRASLADO DE SOPORTES FÍSICOS** 28](#_Toc81624613)

[A9 CONTROL DE ACCESO 29](#_Toc81624614)

[OBJETIVO 1: REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO 30](#_Toc81624615)

[**9.1.1 POLÍTICA DE CONTROL DE ACCESO** 30](#_Toc81624616)

[**9.2.2 GESTIÓN DE ACCESO A LOS USUARIOS** 34](#_Toc81624617)

[OBJETIVO 2 GESTIÓN DEL ACCESO DE USUARIOS 36](#_Toc81624618)

[**9.2.1 REGISTRO DE USUARIOS Y CANCELACIÓN DEL REGISTRO** 36](#_Toc81624619)

[**9.2.2 GESTIÓN DE ACCESO A LOS USUARIOS** 36](#_Toc81624620)

[**9.2.3 GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADOS** 37](#_Toc81624621)

[**9.2.4 GESTIÓN DE LA INFORMACIÓN DE AUTENTICACIÓN SECRETA DE LOS USUARIOS** 37](#_Toc81624622)

[**9.2.5 REVISIÓN DE DERECHOS DE ACCESO DE USUARIO** 38](#_Toc81624623)

[**9.2.6 REMOCIÓN O AJUSTE DE LOS DERECHOS DE ACCESO** 38](#_Toc81624624)

[OBJETIVO 3: RESPONSABILIDADES DEL USUARIO 39](#_Toc81624625)

[**9.3.1 USO DE LA INFORMACIÓN DE AUTENTICACIÓN SECRETA** 39](#_Toc81624626)

[OBJETIVO 4: CONTROL DE ACCESO AL SISTEMA Y A LAS APLICACIONES 39](#_Toc81624627)

[**9.4.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN.** 39](#_Toc81624628)

[**9.4.2 PROCEDIMIENTOS DE CONEXIÓN (LOG-ON) SEGUROS** 40](#_Toc81624629)

[**9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS** 41](#_Toc81624630)

[**9.4.4 USO DE PROGRAMAS DE UTILIDAD PRIVILEGIADOS** 42](#_Toc81624631)

[**9.4.5 CONTROL DE ACCESO AL CÓDIGO DE PROGRAMAS FUENTE** 42](#_Toc81624632)

[A10 CRIPTOGRAFIA 43](#_Toc81624633)

[OBJETIVO 1: CONTROLES CRIPTOGRÁFICOS 43](#_Toc81624634)

[**10.1.1 POLÍTICA SOBRE EL EMPLEO DE CONTROLES CRIPTOGRÁFICOS** 43](#_Toc81624635)

[**10.1.2 GESTIÓN DE CLAVES** 44](#_Toc81624636)

[A11 SEGURIDAD FISICA Y DEL ENTORNO 45](#_Toc81624637)

[OBJETIVO 1: ÁREAS SEGURAS 46](#_Toc81624638)

[**11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA** 46](#_Toc81624639)

[**11.1.2 CONTROLES DE ACCESO FÍSICO** 50](#_Toc81624640)

[**11.1.3 SEGURIDAD DE OFICINAS, DESPACHOS E INSTALACIONES** 51](#_Toc81624641)

[**11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y DEL AMBIENTE** 51](#_Toc81624642)

[**11.1.5 EL TRABAJO EN LAS ÁREAS SEGURAS** 52](#_Toc81624643)

[**11.1.6 ÁREAS DE ENTREGA Y DE CARGA** 52](#_Toc81624644)

[OBJETIVO2: SEGURIDAD DE LOS EQUIPOS 53](#_Toc81624645)

[**11.2.1 UBICACIÓN Y PROTECCIÓN DEL EQUIPAMIENTO** 53](#_Toc81624646)

[**11.2.2 ELEMENTOS DE SOPORTE** 53](#_Toc81624647)

[**11.2.3 SEGURIDAD EN EL CABLEADO** 54](#_Toc81624648)

[**11.2.4 MANTENIMIENTO DEL EQUIPAMIENTO** 55](#_Toc81624649)

[**11.2.5 RETIRO DE BIENES** 56](#_Toc81624650)

[**11.2.6 SEGURIDAD DEL EQUIPAMIENTO Y DE LOS ACTIVOS FUERA DE LAS INSTALACIONES** 56](#_Toc81624651)

[**11.2.7 SEGURIDAD EN LA REUTILIZACIÓN O ELIMINACIÓN DE EQUIPOS** 56](#_Toc81624652)

[**11.2.8 EQUIPAMIENTO DESATENDIDO POR EL USUARIO** 56](#_Toc81624653)

[**11.2.9 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS** 57](#_Toc81624654)

[A12 SEGURIDAD DE LAS OPERACIONES 58](#_Toc81624655)

[OBJETIVO 1: PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES 59](#_Toc81624656)

[**12.1.1 PROCEDIMIENTOS DOCUMENTADOS DE OPERACIÓN** 60](#_Toc81624657)

[**12.1.2 GESTIÓN DE CAMBIOS** 61](#_Toc81624658)

[**12.1.3 GESTIÓN DE LA CAPACIDAD** 62](#_Toc81624659)

[**12.1.4 SEPARACIÓN DE LOS AMBIENTES PARA DESARROLLO, PRUEBA Y OPERACIÓN** 62](#_Toc81624660)

[OBJETIVO2: PROTECCIÓN ANTE SOFTWARE MALICIOSO 63](#_Toc81624661)

[**12.2.1 CONTROLES ANTE SOFTWARE MALICIOSO** 63](#_Toc81624662)

[OBJETIVO 3 RESPALDO - COPIAS DE SEGURIDAD 65](#_Toc81624663)

[**12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACIÓN** 66](#_Toc81624664)

[OBJETIVO 4 REGISTROS Y SUPERVISIÓN 68](#_Toc81624665)

[**12.4.1 REGISTRO DE EVENTOS** 68](#_Toc81624666)

[**12.4.2 PROTECCIÓN DE LA INFORMACIÓN DE REGISTROS (LOGS)** 69](#_Toc81624667)

[**12.4.3 REGISTROS DEL ADMINISTRADOR Y OPERADOR** 69](#_Toc81624668)

[**12.4.4 SINCRONIZACIÓN DE RELOJES** 70](#_Toc81624669)

[OBJETIVO 5 CONTROL DE SOFTWARE EN LA PRODUCCIÓN 70](#_Toc81624670)

[**12.5.1 INSTALACIÓN DE SOFTWARE EN LOS SISTEMAS OPERATIVOS** 70](#_Toc81624671)

[OBJETIVO 6 GESTIÓN DE VULNERABILIDAD TÉCNICA 71](#_Toc81624672)

[**12.6.1 GESTIÓN DE VULNERABILIDADES TÉCNICAS** 71](#_Toc81624673)

[**12.6.2 RESTRICCIONES EN LA INSTALACIÓN DE SOFTWARE** 73](#_Toc81624674)

[**OBJETIVO 7 CONSIDERACIONES SOBRE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN** 73](#_Toc81624675)

[**12.7.1 CONTROLES DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN** 74](#_Toc81624676)

[A13 SEGURIDAD EN LAS COMUNICACIONES 75](#_Toc81624677)

[OBJETIVO 1: GESTIÓN DE LA SEGURIDAD DE RED 76](#_Toc81624678)

[**13.1.1 CONTROLES DE RED** 76](#_Toc81624679)

[**13.1.2 SEGURIDAD DE LOS SERVICIOS DE RED** 77](#_Toc81624680)

[**13.1.3 SEPARACIÓN EN REDES** 78](#_Toc81624681)

[OBJETIVO2 INTERCAMBIO DE INFORMACIÓN 78](#_Toc81624682)

[**13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACIÓN** 78](#_Toc81624683)

[**13.2.2 ACUERDOS DE INTERCAMBIO DE INFORMACIÓN** 79](#_Toc81624684)

[**13.2.3 MENSAJERÍA ELECTRÓNICA** 79](#_Toc81624685)

[**13.2.4 ACUERDOS DE CONFIDENCIALIDAD Y DE NO DIVULGACIÓN** 80](#_Toc81624686)

[A14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN 81](#_Toc81624687)

[OBJETIVO 1: REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN 82](#_Toc81624688)

[**14.1.1 ANÁLISIS Y ESPECIFICACIÓN DE LOS REQUISITOS DE SEGURIDAD** 82](#_Toc81624689)

[**14.1.2 ASEGURAMIENTO DE LOS SERVICIOS DE APLICACIÓN EN LAS REDES PÚBLICAS** 84](#_Toc81624690)

[**14.1.3 TRANSACCIONES EN LÍNEA** 84](#_Toc81624691)

[OBJETIVO 2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE 85](#_Toc81624692)

[**14.2.1 POLÍTICA DE DESARROLLO SEGURO** 85](#_Toc81624693)

[**14.2.2 PROCEDIMIENTO DE CONTROL DE CAMBIO DEL SISTEMA** 86](#_Toc81624694)

[**14.2.3 REVISIÓN TÉCNICA DE APLICACIONES DESPUÉS DE CAMBIOS DE LAS PLATAFORMAS OPERATIVAS** 87](#_Toc81624695)

[**14.2.4 RESTRICCIONES A LOS CAMBIOS EN LOS PAQUETES DE SOFTWARE** 87](#_Toc81624696)

[**14.2.5 PRINCIPIOS DE LA INGENIERÍA DE SISTEMAS SEGUROS** 88](#_Toc81624697)

[**14.2.6 AMBIENTE DE DESARROLLO SEGURO** 88](#_Toc81624698)

[**14.2.7 DESARROLLO SUBCONTRATADO** 89](#_Toc81624699)

[**14.2.8 PRUEBAS DE SEGURIDAD DEL SISTEMA** 89](#_Toc81624700)

[**14.2.9 PRUEBAS DE ACEPTACIÓN DEL SISTEMA** 89](#_Toc81624701)

[OBJETIVO 3 DATOS DE PRUEBA 90](#_Toc81624702)

[**14.3.1 PROTECCIÓN DE DATOS DE PRUEBA** 90](#_Toc81624703)

[A15 RELACION CON PROVEEDORES 90](#_Toc81624704)

[OBJETIVO 1: SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES 91](#_Toc81624705)

[**15.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES** 92](#_Toc81624706)

[**15.1.2 TENER EN CUENTA LA SEGURIDAD EN LOS ACUERDOS CON PROVEEDORES** 97](#_Toc81624707)

[**15.1.3 CADENA DE SUMINISTRO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES** 106](#_Toc81624708)

[OBJETIVO 2 GESTIÓN DE LA ENTREGA DEL SERVICIO POR TERCERAS PARTES 108](#_Toc81624709)

[**15.2.1 SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE PROVEEDORES** 108](#_Toc81624710)

[**15.2.2 GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES** 108](#_Toc81624711)

[A16 GESTION DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACION 109](#_Toc81624712)

[OBJETIVO 1: GESTIÓN DE INCIDENTES Y MEJORAS DE SEGURIDAD DE LA INFORMACIÓN 110](#_Toc81624713)

[16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS 111](#_Toc81624714)

[16.1.2 REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN 112](#_Toc81624715)

[16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN 115](#_Toc81624716)

[16.1.4 EVALUACIÓN Y DECISIÓN SOBRE LOS EVENTOS DE SEGURIDAD DE INFORMACIÓN 116](#_Toc81624717)

[16.1.5 RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 117](#_Toc81624718)

[16.1.6 APRENDIENDO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 117](#_Toc81624719)

[16.1.7 RECOLECCIÓN DE EVIDENCIA 118](#_Toc81624720)

[A17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO 120](#_Toc81624721)

[OBJETIVO 1: CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN 123](#_Toc81624722)

[**17.1.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN** 123](#_Toc81624723)

[**17.1.2 IMPLEMENTACIÓN DE LA CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN** 124](#_Toc81624724)

[**17.1.3 VERIFICAR, REVISAR Y EVALUAR LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN** 126](#_Toc81624725)

[OBJETIVO 2: REDUNDANCIA 128](#_Toc81624726)

[**17.2.1 DISPONIBILIDAD DE LAS INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN** 128](#_Toc81624727)

[A18 CUMPLIMIENTO 129](#_Toc81624728)

[OBJETIVO 1: CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES 130](#_Toc81624729)

[**18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES** 131](#_Toc81624730)

[**18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL (/PR)** 131](#_Toc81624731)

[**18.1.3 PROTECCIÓN DE LOS REGISTROS** 132](#_Toc81624732)

[**18.1.4 PROTECCIÓN DE LOS DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL** 133](#_Toc81624733)

[**18.1.5 REGULACIÓN DE LOS CONTROLES CRIPTOGRÁFICOS** 133](#_Toc81624734)

[OBJETIVO.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN 135](#_Toc81624735)

[**18.2.1 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN** 135](#_Toc81624736)

[**18.2.2 CUMPLIMIENTO DE LA POLÍTICA Y LAS NORMAS DE SEGURIDAD** 136](#_Toc81624737)

[**18.2.3 REVISIÓN DEL CUMPLIMIENTO TÉCNICO** 136](#_Toc81624738)

**A5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**

Citando la norma ISO 27001:

**Objetivo 1:**  
Proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes

**Controles:**

* **5.1.1 Políticas para la seguridad de la información**
* **5.1.2 Revisión de las políticas de seguridad de la información**

**5.1.1 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN**

Este control requiere que se definan políticas de la seguridad de la información:

* Sean aprobadas por la dirección
* Deben publicarse y comunicarse a los empleados y partes externas pertinentes

*Una buena recomendación*

*La comunicación de las políticas debe realizarse a todos los niveles, no solo al nivel de los directivos y responsables*

*El objetivo de la Seguridad de la información pasa por involucrar a toda la organización en esta tarea*

*En el apartado Comunicación y sensibilización en el SGSI encontrara información valiosa para abordar este punto tan importante*

Algunos ejemplos de políticas de Seguridad pueden ser:

* Política de control de acceso
* Política de clasificación y manejo de la información
* Política de seguridad física y ambiental (ver 11)
* Política de temas finales orientados al usuario, tales como:
  + Política de uso aceptable de activos
  + Política de escritorio y pantalla limpios
  + Política de transferencia de información
  + Política de dispositivos móviles y teletrabajo
  + Política de restricciones a las instalaciones y uso del software
  + Política de copia de seguridad
  + Política de transferencia de información
  + Política de protección contra software malicioso
  + Política de gestión de vulnerabilidades
  + Política de controles criptográficos
  + Política de seguridad de las comunicaciones
  + Política de privacidad y protección de la información personal identificable
  + Política de relación con los proveedores

**5.1.2 REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**

Las políticas de la Seguridad de la información deben adaptarse continuamente a las necesidades y cambios de la organización por lo que no pueden permanecer estáticas.

Se trata entonces de mantener actualizada la política de la seguridad de la información. Para ello es interesante tener en cuenta algunas recomendaciones

***ALGUNOS CONSEJOS PRÁCTICOS***

*Desarrollar una política con distintos documentos con una estructura jerárquica:*

* ***Una política general de la alta dirección para expresar el compromiso de toda la organización con la seguridad de la información***
* ***Otras políticas definidas por departamentos o áreas de la organización***
* ***Instrucciones técnicas o documentos de aplicabilidad de las políticas definidas en las políticas especificas***

**A6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**

Citando la norma **ISO 27001**:

**Objetivo 1:**  
ORGANIZACIÓN INTERNA

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

**Controles:**

* **6.1.1 Funciones y responsabilidades de la Seguridad de la información**
* **6.1.2 Separación de funciones**
* **6.1.3 Contacto con autoridades**
* **6.1.4 Contacto con grupos de interés especial**
* **6.1.5 Seguridad de la información en la gestión de proyectos**

**Objetivo 2:**  
DISPOSITIVOS MÓVILES Y TELETRABAJO

Garantizar la seguridad del teletrabajo y del uso de dispositivos móviles.

**Controles:**

* **6.2.1 Política de dispositivos móviles**
* **6.2.2 Teletrabajo**

**6.1 ORGANIZACIÓN INTERNA**

Aquí se nos presentan una serie de requisitos o controles para garantizar que la organización organice las funciones y responsabilidades para gestionar la seguridad de la información

**6.1.1 FUNCIONES Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN**

Se trata de que deberemos definir las responsabilidades de cada empleado o puesto de trabajo en relación a la Seguridad de la información. Es decir para cumplir con este control bastaría con sumar a las funciones de cada puesto aquellas funciones que tengan que ver con la seguridad de la información (si es pertinente)

Pero no basta con definirlas, también deberemos comunicar a cada persona implicada en la Seguridad de la Información sus roles y responsabilidades

Incluir a terceras partes

Para terminar de cumplir con este control siempre que sea aplicable, deberemos procurar hacer partícipes de las responsabilidades a las partes externas que sean pertinentes tales como

* Usuarios externos
* Proveedores
* Etc.

**6.1.2 SEGREGACIÓN DE TAREAS**

Se trata de evitar usos o accesos indebidos a la información o a las aplicaciones o sistemas que la gestionan (activos de información) mediante la separación de las funciones asignando distintos perfiles o áreas de responsabilidad

Explicado de otra forma, podemos determinar las responsabilidades, tareas, accesos, etc. que conllevan un riesgo de mal uso, accidental o deliberado, si son compartidas por una misma persona

CASO PRACTICO:  
Ejemplos de separación o segregación de responsabilidades (ISO 27002)

* En el proceso de compras deberíamos separar las responsabilidad de quien hace los pedidos y de quien los aprueba o realiza los pagos para evitar el riesgo de fraude o pedidos innecesarios o en desacuerdo con las políticas de compras.
* Evitar que personal de desarrollo tenga acceso administrativo a los sistemas en producción evitara el riesgo de usos indebidos de aplicaciones que deben controlar solamente aquellas personas autorizadas a administrar sistemas con clientes reales
* Separar las funciones de petición y concesión de permisos administrativos de acceso a sistemas o áreas restringidas evitando que la misma persona que realiza las solicitudes de acceso sea quien se concede las autorizaciones o maneja la asignación de contraseñas de acceso

**Alternativas a la segregación de funciones**

A veces por motivos de costes no podemos diferenciar las responsabilidades o tareas. Entonces la pregunta es ¿qué podemos hacer si nuestra empresa es demasiado pequeña y no tenemos más remedio que concentrar funciones en las mismas personas?

La alternativa está en establecer controles que mitiguen los riesgos provocados por la imposibilidad práctica de segregar las funciones

Estos pueden ser:

**Controles de seguimiento y monitorización:**

Establecer controles de supervisión de las actividades en tiempo real puede darnos mayor seguridad de que se realizan correctamente

**Controles de Auditorias**

Establecer controles mediante registros que revelen los datos necesarios en las auditorias periódicas para evaluar las posibles violaciones de seguridad. También es aconsejable aumentar la frecuencia de las auditorias en temas sensibles con el objeto de transmitir a los empleados la continuidad en la vigilancia de la seguridad de la información

**Registros automatizados**

Registrar de forma automática los cambios, accesos o tareas sensibles con la seguridad de la información como la asignación de permisos, contraseñas o modificaciones en aplicaciones de desarrollo

**6.1.3 CONTACTO CON AUTORIDADES**

En caso de incidentes en la seguridad de la información puede resultar necesario mantener informados a los organismos de control del estado o administración. Estos pueden ser comúnmente

* Agencia de protección de datos
* Fuerzas y Cuerpos de seguridad del estado
* Otros

Este control debe ser implementado en caso de empresas u organizaciones:

* Grandes empresas que mantienen servicios particularmente relevantes para al ámbito público, telecomunicaciones, organizaciones bancarias, servicios de emergencia etc.
* Empresas más pequeñas que manejen datos sensibles y cuya difusión indebida o robo pueda causar daños a las personas involucradas
* Cuando los incidentes contra la seguridad de la información provienen de una fuente externa como Internet y resulte útil o necesario que varias autoridades y proveedores deban ser llamados a la acción para desviar, suprimir o mitigar la amenaza.

**6.1.4 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL.**

Mantenerse al día en Seguridad de la información parece una tarea imposible de realizar de forma autónoma aun para grandes corporaciones por lo que este control nos indica que deberemos identificar todos aquellos grupos de interés tales como: foros especializados en Seguridad de la información, organismos o empresas expertas en seguridad de la información.

Se trata de mantenernos actualizados en cuanto a las noticias sobre la seguridad de la información y permanecer alerta ante las nuevas amenazas para la seguridad de la información y si es necesario que adoptemos alguna recomendación de estos grupos especializados.

**6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.**

Este control es algo totalmente novedoso en ISO 27001 por lo que intentaremos darle la información oportuna para saber interpretar este requisito

**INTEGRAR LA SEGURIDAD EN LOS PROCESOS DE LA ORGANIZACIÓN**

Este control pretende decirnos que la Seguridad de la Información debe involucrarse en todos los procesos de la organización ya sean procesos del Negocio, procesos internos, Servicios o productos, Procesos TI etc.

***¿En qué consiste esto de considerar la seguridad de la información en todos los procesos?***

Partamos de la base de que la seguridad es algo que generalmente se olvida en los proyectos; es decir, cuando un proyecto se aborda en una organización, generalmente no tiene en cuenta la seguridad de la información.

Para afrontar este requisito bastaría con realizar una evaluación de riesgos, centrada en la seguridad de la información, al comienzo de cualquier proyecto para identificar amenazas, vulnerabilidades y riesgos asociados al proyecto. Esto nos permitirá adoptar los controles necesarios.

Con esto cumplimos con lo que dice la norma:

*La seguridad de la información debe abordarse en la gestión de proyectos, independientemente del tipo de proyecto.*

Si queremos ser más rigurosos podemos establecer un proceso para integrar la Seguridad de la información en cualquier proyecto:

**PASO1 Objetivos de Seguridad**  
Plantearse como una actividad más dentro de las actividades de cualquier proyecto de cara a determinar los objetivos de para preservar la confidencialidad, integridad y disponibilidad de la información relacionada o afectada por el proyecto

**PASO2 Evaluación de riesgos**  
En la fase de diseño o planificación del proyecto se puede realizar un análisis de riesgos que nos permita identificar y ponderar los riesgos asociados a la seguridad de la información

**PASO3 Controles de seguridad**  
La evaluación de riesgos nos permitirá tomar las decisiones adecuadas para establecer los controles necesarios para mitigar los riesgos

**PASO4 Proceso de Seguridad de la Información**  
Una vez que hemos realizado un ejercicio según los pasos anteriores podemos entonces establecer un proceso documentado para integrar la seguridad de la información en cualquier proceso con el conocimiento de lo que hemos aprendido

Beneficios de la integración de la Seguridad de la Información

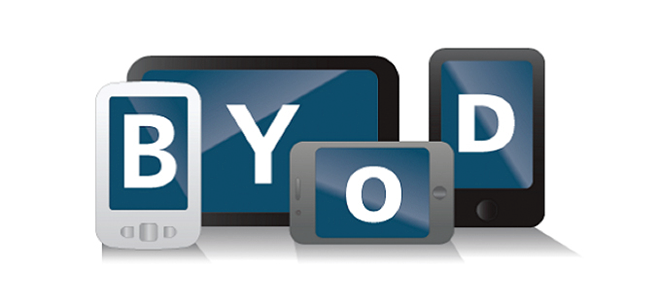
* Cumplir con los requisitos de la norma
* La consideración de la Seguridad de la información en todos los proyectos otorgara un mayor valor a todos sus proyectos y a toda la organización
* Mejora la evaluación de costes de un proyecto al considerar anticipadamente riesgos, que después pueden suponer costes no evaluados

**6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO**

El objetivo de este apartado es poder garantizar la seguridad en dispositivos móviles y en las condiciones del teletrabajo.

**6.2.1 POLÍTICA DE DISPOSITIVOS MÓVILES**

Se trata de que dispongamos de políticas de Seguridad de la Información como medidas concretas que mitiguen los riesgos de la seguridad de la información en el uso de dispositivos móviles en una organización



El requisito que nos pide la norma es que seamos capaces de demostrar que hemos adoptado políticas, respaldadas por medidas o los controles de seguridad para reducir el riesgo que representan los dispositivos móviles o remotos

La política de uso de dispositivos móviles en una organización debe considerar:

* El registro de nuevos dispositivos
* La cancelación de registro de dispositivos móviles
* Requisitos de seguridad física
* Requisitos de seguridad técnica incluidas conexiones remotas
* Control de software
* Control de acceso y encriptación en reposo y de dispositivos en tránsito.

Las políticas diseñadas para dispositivos móviles además de los requisitos anteriores deberían considerar las condiciones de uso de dispositivos móviles y cuando sean apropiados.

**Dispositivos BYOD**

Según leemos los requisitos descritos hasta ahora podemos deducir que naturalmente estamos hablando de dispositivos móviles administrados.

Pero entonces ¿Qué pasa con los dispositivos propios de los empleados o de agentes externos que se utilizan dentro de los ambientes de trabajo y se conectan a las redes LAN, WiFi, a los servicios de correo etc.?

Estos dispositivos son los denominados BYOD (Bring your own device - Usa tu propio dispositivo)

Desde luego este tema es un tema bastante actual y “candente” para la seguridad de la información, y muchos profesionales están de acuerdo en que los riesgos que suponen los dispositivos no administrados y de propiedad personal son demasiado grandes.

Sin embargo, ISO 27001 no específica si los dispositivos no administrados (BYOD) están permitidos o no; simplemente requiere que la organización lo determine mediante una política las condiciones de uso para estos dispositivos y debe supervisar el cumplimiento de esta política a través de auditorías o controles técnicos.

**6.2.2 TELETRABAJO**

En la actualidad el teletrabajo es una actividad tremendamente difundida en todo tipo de organizaciones por lo que la seguridad de la Información es un aspecto clave para garantizar la protección de esta actividad

Una vez más se trata de:

* Evaluar que activos de información están involucrados en el teletrabajo
* Realizar una evaluación de riesgos aplicada a los activos de la información y a las actividades del teletrabajo
* Aplicar los controles adecuados para mitigar los riesgos identificados

Quizás para pequeñas empresas o empresa con infraestructuras de TI relativamente sencilla, las medidas de seguridad pueden consistir en la restricción del acceso a determinados activos

Para organizaciones de mayor complejidad la norma nos provee de una serie de controles a tener en cuenta en el análisis de aplicabilidad:

Citando la norma:

*"Restricciones o controles para actividades de Teletrabajo según ISO 27002"*

* La seguridad física existente del sitio de teletrabajo, considerando la seguridad física del edificio y del entorno local;
* El entorno físico de teletrabajo propuesto;
* Los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a ser accedida y pasada sobre el enlace de comunicación y la sensibilidad! del sistema interno;
* la provisión de acceso al escritorio virtual que impide el procesamiento y el almacenamiento de información sobre el equipo de propiedad privada;
* la amenaza de acceso no autorizado a la información o a los recursos de otras personas que utilizan el alojamiento, por ejemplo, familiares y amigos;
* el uso de redes domésticas y requisitos o restricciones de la configuración de los servicios de red inalámbricos;
* las políticas y los procedimientos para evitar conflictos relativos a los derechos de propiedad intelectual desarrollados en los equipos de propiedad privada;
* el acceso a los equipos de propiedad privada (para verificar la seguridad de la máquina durante la investigación), que puede ser prevenido por la legislación;
* Los acuerdos de licencia de licencia software que son tales que, las organizaciones pueden ser responsables de la concesión de licencias a los clientes de software en estaciones de trabajo de propiedad privada de. Los empleados o de usuarios de terceras partes;
* La protección ante software malicioso y los requisitos de firewall

La norma nos propone además una lista de aspectos a considerar en la definición de las normas o reglas de aplicación del teletrabajo

Citando la norma:

*" Restricciones o controles para actividades de Teletrabajo según ISO 27002"*

* el suministro de equipo adecuado y mobiliario de almacenamiento para las actividades de teletrabajo, donde no se permite el uso de equipo de propiedad privada, que no se encuentra bajo control de la organización;
* Una definición del trabajo permitido, las horas de trabajo, la clasificación de la información que se puede realizar y los sistemas y servicios internos a los que el teletrabajador se encuentra autorizado a acceder;
* El suministro de equipo adecuado de comunicación, incluyendo los métodos para asegurar el acceso remoto;
* La seguridad física;
* Las reglas y directrices del acceso de la familia y visitas al equipo y la información;
* El suministro de soporte y mantenimiento de hardware y software;
* La provisión de seguros;
* Los procedimientos para el respaldo y la continuidad del negocio;
* La auditoría y el control de la seguridad;
* La revocación de la autoridad y de los derechos de acceso, y el regreso de los equipos cuando las actividades de teletrabajo finalizan.

**A7 SEGURIDAD RELATIVA A LOS RECURSOS**

Por un lado las personas son el activo más importante en una organización pero a su vez podemos considerar que los errores humanos son normalmente el mayor riesgo para la seguridad de la información

Los controles para la seguridad de la información que se consideran en este capítulo de ISO 27001 abordan las medidas para la seguridad a abordar en la fase de contratación, durante el empleo y en la fase de término o finalización del empleo

Citando la norma:

**Objetivo 1:**  
PREVIO AL EMPLEO

Asegurar que los empleados y contratistas entiendan sus responsabilidades y que sean aptos para los roles para los cuales están siendo considerados

**Controles:**

* **7.1.1 Selección**
* **7.1.2 Términos y condiciones de empleo**

**Objetivo 2:**  
Durante el empleo

Asegurar que los empleados y contratistas sean conscientes de y cumplan con las responsabilidades de seguridad de la información

**Controles:**

* **7.2.1 Responsabilidades de la dirección**
* **7.2.2 Concientización, educación y formación en seguridad de la información**
* **7.2.3 Proceso disciplinario**

**Objetivo 3:**  
Finalización o cambio de la relación laboral o empleo

**Controles:**

* **7.3.1 Responsabilidades en la desvinculación**

**7.1 PREVIO AL EMPLEO**

Se establecen controles para la verificación de los antecedentes de los candidatos a un empleo. La aplicabilidad de este control tiene que ver con:

* Los requisitos del negocio en cuanto a las funciones que va a desempeñar el candidato y los requisitos definidos para el puesto en relación a la Seguridad de la información
* La clasificación de la información a la que va acceder el candidato y los riesgos asociados

Una de las limitaciones para implementar este control son las leyes o normas vigentes relacionadas con la protección de datos personales y el tratamiento ético en los contratos.

Vamos ver los controles con detalle

**7.1.1 SELECCIÓN**

En el proceso de selección podremos aplicar una serie de controles para verificar temas de seguridad así como la formación y experiencia del contrato. El tema es simple, La norma nos propone una serie de medidas para que evaluemos la necesidad de aplicarlas

Medidas de Seguridad den el proceso de Selección de personal

* Comprobar si existen referencias satisfactorias tanto en el ámbito profesional como en el personal
* Comprobar la veracidad del currículum vitae del postulante;
* Confirmar las calificaciones académicas y profesionales declaradas;
* Comprobar de forma independiente la identidad (pasaporte DNI etc.)
* Comprobaciones en detalle: Deudas, antecedentes penales etc.

Competencias en Seguridad de la información

* Comprobar si tiene la capacitación necesaria para desempeñar sus funciones (Formación, experiencia)
* Verificar en lo posible el perfil del candidato en relación a su confiabilidad si va a desempeñar una tarea sensible para la organización en materia de Seguridad de la Información

**CONTRATISTAS**

Igualmente podemos establecer controles similares antes de firmar contratos con terceros

**PROCESOS DE PROMOCION**

Los procesos de selección no solo tienen que ver con contratación de personal nuevo sino que también podemos aplicar medidas para la seguridad de la información análogas en los procesos de promoción dentro de la organización

**7.1.2 TÉRMINOS Y CONDICIONES DE EMPLEO**

Este control nos pide incluir en los contratos con los empleados y subcontratas las obligaciones y responsabilidades ligadas a la Seguridad de la Información

Quizás no sea totalmente disuasorio, pero teniendo en cuenta que muchos de los comportamientos anómalos dentro de una organización son debidos a relajación de las propia organización, el mantener informados a los trabajadores de las condiciones de trabajo es una muy buena medida preventiva de conductas indebidas para la seguridad de la información.

Tenga en cuenta que en las primeras etapas de un contrato no se producen normalmente violaciones a las políticas de seguridad, pero con el tiempo las diversas circunstancias particulares pueden ser desencadenantes de conductas no apropiadas.

La norma nos propone algunas medidas concretas que deberíamos tomar si son aplicables:

* Todos los empleados y contratistas con acceso a información sensible deben firmar acuerdos de confidencialidad o de no divulgación antes de que tengan los permisos para acceder a dicha información
* Los empleados y contratistas deben estar informados de sus responsabilidades y derechos legales tales como las relativas a derecho de copia o legislación de protección de datos
* Los empleados y contratistas deben tener información de sus responsabilidades para
* La clasificación de información
  + La gestión de activos de información
  + Las instalaciones de procesamiento de información
  + Los servicios de información a los que accede
  + El manejo de información de otras organizaciones o partes externas
* Los empleados y contratistas deben estar informados de las acciones a ser tomadas si el empleado o contratista desatiende los requisitos de la seguridad de la organización

**7.2 DURANTE EL EMPLEO**

También deberemos asegurarnos de que durante el desempeño de las funciones o actividades cada empleado conozca y cumpla con sus obligaciones y tareas asignadas relativas a la Seguridad de la Información

Para ello se nos proponen los siguientes controles

**7.2.1 RESPONSABILIDADES DE LA DIRECCIÓN**

Este apartado responde a la pregunta del auditor:

***¿De qué forma la dirección les exige a los empleados que cumplan con las políticas, normas y procedimientos establecidos para la Seguridad de la Información?***

La norma nos incluye los siguientes puntos para cumplir con este control

* ¿Se ha formado y capacitado a los empleados en sus responsabilidades sobre la seguridad de la Información antes de que tengan acceso a los activos de información?
* ¿Se les ha informado de los resultados que la organización espera de sus funciones en relación a la seguridad de la información?
* ¿Se ha motivado y concienciado suficientemente a los empleados para que cumplan con sus obligaciones en las tareas de la Seguridad de la información?
* ¿Se ha obtenido un feedback del acuerdo de los trabajadores con los métodos de trabajo seguros y la parte que les afecta de las políticas de la seguridad de la información?
* ¿Se realiza un proceso de formación continua para mantener las habilidades en el desarrollo de las tareas de la Seguridad de la Información?
* ¿Existe un canal de información que garantice el anonimato para denunciar los fallos y violaciones a las normas sobre la Seguridad de la Información?

**7.2.2 CONCIENTIZACIÓN, EDUCACIÓN Y FORMACIÓN EN SEGURIDAD DE LA INFORMACIÓN**

Citando la norma:

*"Todos los empleados de la organización y, cuando sea pertinente, contratistas, deberían recibir concientización, entrenamiento y formación adecuada y actualizaciones regulares en políticas y procedimientos organizacionales, relevantes para su función laboral."*

La norma nos da algunas indicaciones de aspectos que deben incluirse en la formación y sensibilización

* La formación debe incluir el compromiso de la dirección con la seguridad de la información en toda la organización
* La importancia del conocimiento y el cumplimiento de las obligaciones aplicables de seguridad de la información contenida en las políticas, normas, contratos etc.
* La responsabilidad de los empleados y contratistas de sus propias acciones u omisiones en la protección de la información
* Los procedimientos básicos de la seguridad de la información, por ejemplo:
  + Procedimiento de notificación de incidentes de seguridad
  + Procedimientos sobre uso de contraseñas seguras
  + Controles sobre software malicioso
  + Limpieza de escritorios
  + Etc.

Los recursos que disponen para obtener más información sobre cuestiones de la seguridad de la información (puntos de contacto, manuales o especificaciones etc.)

**7.2.3 PROCESO DISCIPLINARIO**

Este control nos propone implantar un sistema disciplinario para los incumplimientos de la seguridad de la información. Un procedimiento que sea formal y comunicado a los empleados

El proceso disciplinario debería:

* Asegurarse de que la infracción se ha cometido
* Evitar tratamientos injustos o incorrectos de los empleados
* Considerar respuestas graduales tomando en cuenta la gravedad, el impacto, si es deliberada o si existe repetición

**NOTA:** un sistema disciplinario no siempre tiene que tener medidas correctivas o negativas. También podemos considerar un sistema disciplinario con medidas positivas que premien el buen desempeño o se establezcan sistemas de que involucren a los empleados (competiciones, gamificación etc.)

**7.3 FINALIZACIÓN O CAMBIO DE LA RELACIÓN LABORAL O EMPLEO**

El objetivo es el de proteger la información en un escenario de finalización de contrato o cambio de empleo

Esta es una parte que lamentablemente se pasa por alto en numerosas organizaciones y que tiene un importante potencial de riesgo para la seguridad de la información y que debemos considerar dentro de un SGSI

**7.3.1 RESPONSABILIDADES EN LA DESVINCULACIÓN**

Se trata de establecer y comunicar al empleado las responsabilidades sobre la seguridad de la información después de finalizar un contrato o ante el cambio de empleo

La norma nos propone este control que incluye las siguientes cuestiones:

* Incluir en las responsabilidades de la desvinculación requisitos sobre la seguridad de la información tales como
  + Responsabilidades legales cuando sean aplicables o necesarias
  + Responsabilidades incluidas en los acuerdos de confidencialidad
* Establecer periodos de vigencia para después de la desvinculación en los términos y condiciones del empleo de:
  + Deberes y responsabilidades que permanecen validos después de la desvinculación
  + Cambiar o actualizar las responsabilidades en los términos y condiciones del empleo ante cambios de empleo dentro de la organización

**A8 GESTION DE ACTIVOS**

El objetivo de este punto de la norma ISO 27001 es la preservación de los activos de información como soporte del negocio

Citando la norma:

**Objetivo 1:**  
Responsabilidad de los activos

Identificar los activos y definir las responsabilidades de protección adecuadas

**Controles:**

* **8.1.1 Inventario de activos**
* **8.1.2 Propiedad de los activos**
* **8.1.3 Uso aceptable de los activos**
* **8.1.4 Devolución de activos**

**Objetivo 2:**  
Clasificación de la información

Asegurar que la información recibe el nivel de protección adecuado de acuerdo con su importancia en la organización.

**Controles:**

* **8.2.1 Clasificación de la información**
* **8.2.2 Etiquetado de la información**
* **8.2.3 Manejo de los activos**

**Objetivo 3:**  
Manejo de los Soportes

* **8.3.1 Gestión de Soportes extraíbles**
* **8.3.2 Eliminación de Soportes**
* **8.3.3 Traslado de soportes físicos**

**8.1 RESPONSABILIDAD DE LOS ACTIVOS**

EL objetivo de este punto es la identificación de los activos de información y las responsabilidades sobre los mismos, con el objetivo de evaluar las medidas de protección adecuadas para cada activo en base a una evaluación de riesgos

Los controles para este objetivo son los siguientes:

**8.1.1 INVENTARIO DE ACTIVOS**

Se trata de realizar un inventario de activos que nos permita.

* Identificar los activos de información que dan soporte al negocio
* Clasificar los activos por su importancia
* Clasificar los activos por el tipo de activo o información
* Identificar al propietario del activo

El inventario de activos debe además

Aquí podemos ver información detallada de cómo realizar un inventario de activos de la información

**8.1.2 PROPIEDAD DE LOS ACTIVOS**

Como hemos visto el inventario de activos debe identificar al propietario del activo

Para asignar al propietario de un activo debemos preguntarnos solamente quien crea, gestiona su transferencia, almacenamiento o destrucción del activo, En definitiva, el que gestiona el activo debe ser asignado como propietario

El propietario del activo en ningún caso es el dueño del activo sino el que tiene una serie de responsabilidades sobre el activo, las cuales enumeramos:

Citando la norma:  
Obligaciones del propietario de un activo de información

* Asegurar que los activos son inventariados
* Asegurar que los activos son clasificados y protegidos adecuadamente;
* Definir y revisar periódicamente las restricciones de acceso y las clasificaciones de activos importantes, teniendo en cuenta las políticas aplicables de control de acceso;
* Garantizar el manejo adecuado cuando el activo es eliminado o destruido.

**¿Quién puede ser el propietario de un activo de información?**

El propietario de un activo de información puede ser un individuo o una entidad que a la que la dirección ha asignado la responsabilidad de gestionar el activo en su ciclo de vida completo.

**8.1.3 USO ACEPTABLE DE LOS ACTIVOS**

El uso aceptable de los activos consiste en un proceso de:

* Documentar el uso apropiado de la información describiendo los requisitos de seguridad de la información de los activos, instalaciones etc.
* Comunicar a los empleados afectados para evitar el uso indebido.

CASO PRACTICO:

*El uso aceptable de activos podría incluir medidas relacionadas con la difamación, el acoso, la suplantación de identidad, las cadenas de cartas (especialmente el ransomware) y las compras no autorizadas etc.*

**8.1.4 DEVOLUCIÓN DE ACTIVOS**

Control para que todos los empleados, contratistas etc. devuelvan los activos de información una vez finalizado el periodo de su utilización, contrato o acuerdo.

Requisitos para implementar este control:

* Formalizar el proceso de finalización de uso incluyendo la cláusula de devolución de activos físicos y/o electrónicos
* Establecer procedimientos transferencia y borrado de información de forma segura en el caso que sea pertinente (Uso de equipos propios, transferencia y devolución de equipos etc.)

Una buena recomendación. No se olvide nunca de:

* Controlar la copia no autorizada de información desde el periodo de aviso de finalización hasta que se materializa la devolución y borrado de datos

**8.2 CLASIFICACIÓN DE LA INFORMACIÓN**

**8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN**

La información debería clasificarse según:

* Su valor para la organización
* Los requisitos legales (Datos personales, Sensibles etc.)
* Nivel de Protección necesario: Su criticidad y sensibilidad en cuando a su divulgación o modificación no autorizada o accidental.

Como hemos visto antes el responsable de la clasificación de la información es el responsable del activo

Algunas cosas a tener en cuenta

* El esquema de clasificación debe ser uniforme para toda la empresa
* El esquema de clasificación debe alinearse con la política de control de acceso
* El nivel de protección debe ser evaluado según los criterios de confidencialidad, integridad y disponibilidad
* La clasificación del activo debe revisarse periódicamente y mantenerse actualizada

**Otras consideraciones**

Podríamos agrupar tipos de activos o información con requisitos de protección similares de forma que no tengamos que realizar una especificación de procedimientos de seguridad de la información caso a caso sino para un grupo de activos de información similares

La norma nos proporciona un ejemplo para la clasificación de la criticidad de la información en relación a la confidencialidad

* Nivel 0 la divulgación no causa ningún daño
* Nivel 1 la divulgación causa menor incomodidad o inconveniencia operativa menor;
* Nivel 2 la divulgación tiene un impacto significativo a corto plazo en las operaciones o los objetivos tácticos;
* Nivel 3 la divulgación tiene un grave impacto en los objetivos estratégicos a largo plazo o pone en riesgo la supervivencia de la organización.

**8.2.2 ETIQUETADO DE LA INFORMACIÓN**

La información debería ser etiquetada de acuerdo al esquema de clasificación que hayamos definido en el apartado anterior

**PROCESO O PROCEDIMIENTO DE ETIQUETADO**

El proceso de etiquetado puede tener excepciones (Activos que no necesiten etiquetado. Por ejemplo, podemos evitar tener que poner la etiqueta: “Información no confidencial”), algo que tiene que estar especificado en un procedimiento de etiquetado.

Los activos de los sistemas que contienen información clasificada como sensible o crítica deberían llevar una etiqueta adecuada de clasificación.

El etiquetado de la información clasificada es un requisito clave para acuerdos que impliquen compartir información.

Los requisitos son:

* El etiquetado afecta a la información y sus activos relacionados en formato físico y electrónico.
* Debe realizarse según el esquema de clasificación definido en el punto anterior
* Las etiquetas deben reconocerse fácilmente

El etiquetado de la información puede realizarse de forma física o por medio de metadatos.

Tenga en cuenta que el etiquetado de los activos puede ser un reclamo para el robo de información

**8.2.3 MANEJO DE LOS ACTIVOS**

Este control exige el desarrollo de procedimientos de manejo de activos que tengan en cuenta la clasificación de los activos de información (8.2.1)

Se trata de procedimientos que para:

* el manejo de los activos
* su procesamiento
* el almacenamiento y
* como se debe comunicar de la información

Elementos a tener en cuenta a la hora de definir estos procedimientos

* Considerar las restricciones de acceso derivadas de su nivel de clasificación
* Crear y mantener un registro de autorizaciones de uso o acceso a los activos
* Procedimientos de copias de seguridad para la protección de los activos
* Los procedimientos de almacenamiento de acuerdo las especificaciones del fabricante
* Borrar el marcado de todas las copias en los soportes para la atención del destinatario autorizado

**INTERCAMBIOS DE INFORMACION**

El etiquetado de los activos y de la información no tiene por qué coincidir de una organización a otra por lo que en los procesos de manejo de activos en caso de intercambios de información deberíamos incluir la información sobre la clasificación de la información para interpretar las etiquetas de clasificación de otras organizaciones.

**8.3 MANIPULACIÓN DE SOPORTES**

Se trata de proteger la información en el nivel de soportes en los que se encuentra ya sea papel o soportes electrónicos

**8.3.1 GESTIÓN DE SOPORTES EXTRAÍBLES**

Los soportes extraíbles pueden suponer una brecha importante en la seguridad de la información por lo que la norma propone un control específico para este tipo de soportes



Para gestionar los soportes extraíbles debemos considerar:

* La necesidad de su uso
* los soportes reutilizables que deberían retirarse de la organización y hacerse irrecuperables
* Cuando sea practico debemos requerir autorización para su uso
* Mantener un registro de altas y bajas
* Considerar especificaciones de almacenamiento según especificaciones del fabricante
* Encriptar datos para proteger aquellos que se consideren importantes
* Renovar dispositivos con un periodo determinado para evitar la degradación de datos necesarios e importantes
* Proteger la información almacenada con copias de seguridad en soportes independientes
* Crear un registro de soportes extraíbles para limitar la posibilidad de pérdida de datos
* Controlar la transferencia de información hacia medios extraíbles
* Documentar los procedimientos de autorización

**8.3.2 ELIMINACIÓN DE SOPORTES**

Control:

Establecer procedimientos para la eliminación segura de soportes a la finalización de su uso

Se trata de minimizar o evitar que los datos sensibles o confidenciales puedan ser recuperados una vez que el dispositivo se da de baja mediante procedimientos de eliminación segura

Los requisitos son

* Establecer un proceso de eliminación segura de datos que no permita su recuperación
* Identificar que dispositivos requieren de un proceso de eliminación segura
* Controlar la utilización de empresas externas para la realización de tareas de eliminación segura estableciendo algún tipo de control
* Mantener un registro dispositivos que han sido dados de baja de forma segura por contener información sensible

**8.3.3 TRASLADO DE SOPORTES FÍSICOS**

Se trata de establecer un control para proteger la información cuando los soportes necesitan ser trasladados entre distintas ubicaciones. Para ello deberemos establecer un control sobre

* El registro de salida de los soportes para su cotejamiento con el transportista y el lugar de destino de mismo incluyendo un control de tiempos de transporte
* Control de transportistas (Utilizar transportistas de confianza)
* Mantener una lista de transportistas autorizados
* Controlar la identificación del transportista o mensajero
* Establecer un procedimiento de cifrado cuando sea necesario y posible
* Controlar los embalajes y las condiciones ambientales (Humedad, temperatura, polvo etc.) con las especificaciones del fabricante.

**A9 CONTROL DE ACCESO**

Las medidas de control de accesos de la norma ISO 27001 están orientadas a controlar y monitorizar los accesos a los medios de información de acuerdo a las políticas definidas por la organización.

Citando la norma:

**Objetivo 1:**  
Requisitos de negocio para el control de acceso

Limitar el acceso a la información y a las instalaciones de procesamiento de información.

**Controles:**

* **9.1.1 Política de control de acceso**
* **9.1.2 Acceso a las redes y a los servicios de red**

**Objetivo 2:**  
Gestión del acceso de usuarios

Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios de información.

**Controles:**

* **9.2.1 Registro de usuarios y cancelación del registro**
* **9.2.2 Gestión de acceso a los usuarios**
* **9.2.3 Gestión de derechos de acceso privilegiados**
* **9.2.4 Gestión de la información de autenticación secreta de los usuarios**
* **9.2.5 Revisión de derechos de acceso de usuario**
* **9.2.6 Remoción o ajuste de los derechos de acceso**

**Objetivo 3:**  
Responsabilidades del usuario

Hacer a los usuarios responsables de salvaguardar su información de autenticación.

* **9.3.1 Uso de la información de autenticación secreta**

**Objetivo 4:**  
Responsabilidades del usuario

Impedir el acceso no autorizado a los sistemas y las aplicaciones.

* **9.4.1 Restricción de acceso a la información**
* **9.4.2 Procedimientos de conexión (log-on) seguros**
* **9.4.3 Sistema de gestión de contraseñas**
* **9.4.4 Uso de programas de utilidad privilegiados**
* **9.4.5 Control de acceso al código de programas fuente**

**OBJETIVO 1: REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO**

Para este objetivo de limitar el acceso a la información únicamente personas autorizadas

Tiene los siguientes controles:

**9.1.1 POLÍTICA DE CONTROL DE ACCESO**

Requisitos para definir las reglas de control de acceso a la información, o sea los derechos y restricciones de acceso a la información

El requisito exacto de este punto, especifica la necesidad de establecer, documentar y revisar la política de control de acceso periódicamente, lo que significa que una política documentada es obligatoria.

Los propietarios de los activos son los que deben determinar estas normas o políticas de control de acceso de acuerdo con la política de seguridad de la información y el análisis de riesgos

El principio básico para la elaboración de estas reglas es:

* La asignación de la menor cantidad de privilegios posibles para llevar a cabo una tarea dentro de un sistema de información
* La concesión de esos privilegios solamente por el tiempo que sea necesario para el desarrollo de las tareas

En otra forma de explicarlo, se deben asignar los permisos de acceso limitados solamente a la información necesaria para hacer un trabajo, tanto a nivel físico (accesos a instalaciones o soportes de información), como lógicos (Accesos a aplicaciones).

Aunque nos hemos referido tanto a permisos del tipo lógico como físico, este apartado solamente se refiere a los accesos a nivel lógico aunque ambos deben ir a la par y basarse en los mismos principios.

Otro principio a tener en cuenta en la elaboración de las políticas de control de acceso es el siguiente:

El objetivo de la política de control de acceso debería ser que todo está prohibido a menos que esté expresamente permitido y no al revés

Profundicemos un poco más en todo esto para ver como aplicamos estos principios

**ASIGNACION DE ROLES**

Los roles dentro de un sistema de Información nos informan de lo que un usuario está autorizado a hacer dentro de un sistema y de lo que no le está permitido

CASO PRACTICO:

*Por ejemplo:*

*Un rol de administrador dentro de un sistema de administración de páginas web CMS puede realizar funciones de editar código, instalar aplicaciones, modificar archivos CSS etc., mientras que un rol de colaborador solamente puede editar el contenido en modo texto de sus propios artículos y un rol de usuario registrado solamente puede acceder a visualizar determinados contenidos*

*Como podemos ver Cada rol no solo tiene una serie de privilegios distintos sino que además existe un mayor nivel de riesgo en un Rol de administrador que en un rol de colaborador. Es por ello que el nivel de confianza juega un papel importante en los requisitos que deberemos exigir a dichas funciones en relación a la Seguridad de la Información*

*De esta forma aplicando los principios sobre la asignación de privilegios deberemos hacernos estas preguntas antes de asignar privilegios a un usuario de sistemas de información: a visualizar determinados contenidos*

*Como podemos ver Cada rol no solo tiene una serie de privilegios distintos sino que además existe un mayor nivel de riesgo en un Rol de administrador que en un rol de colaborador. Es por ello que el nivel de confianza juega un papel importante en los requisitos que deberemos exigir a dichas funciones en relación a la Seguridad de la Información*

*De esta forma aplicando los principios sobre la asignación de privilegios deberemos hacernos estas preguntas antes de asignar privilegios a un usuario de sistemas de información:*

* ¿Cuáles son los mínimos privilegios que puedo asignar a un puesto de trabajo con tal que le permita realizar sus tareas?
* ¿Durante cuánto tiempo es necesario que tenga estos privilegios?
* ¿Resulta pactico y es posible asignar estos privilegios solamente durante el tiempo que está realizando los trabajos?

***¿Qué deberíamos incluir en un documento de política de acceso?***

Ya hemos visto que la política debe considerar unos principios generales. Veamos ahora como elaborar en la práctica este documento

En primer lugar deberemos especificar la postura de su organización sobre los privilegios dentro de la política de control de acceso.

CASO PRACTICO:

*Por ejemplo:*

*Un ejemplo de política de control de acceso ISO 27001 puede ser la gestión de los derechos de acceso del usuario donde se detalla el proceso:*

* Emisión de los privilegios o cuentas de usuario
* Modificación de privilegios
* Revocación de privilegios
* Determinación del ciclo de vida del ID de usuario

*Esto sería la documentación de la postura de la organización dentro de esta política específica*

¡Importante!

*La política sobre la seguridad de la información específica la postura de las organizaciones sobre lo que se tolera y lo que no se tolera, por lo tanto, no se trata de un documento de nivel de "cómo hacerlo" sino simplemente un conjunto de requisitos que la empresa debe cumplir.*

*Por ejemplo:*

*“Las cuentas de usuario solo se emitirán después de la aprobación formal de la gerencia de TI y de Recursos Humanos.”*

Otro caso típico no lo encontramos en las reglas que rigen el proceso de emisión de permisos a cuentas de usuarios con altos privilegios. Este tema debería abordarse en una política específica de control de acceso, que está respaldada por procedimientos formales que guíen a los empleados en el proceso a seguir para emitir cuentas privilegiadas.

**9.2.2 GESTIÓN DE ACCESO A LOS USUARIOS**

Se trata de un requisito para la gestionar la autorización de los usuarios que acceden a los recursos de red

Para ello se exige como requisito elaborar una política específica para el uso de los recursos de red

Aunque este requisito o control está cubierto en gran parte por el punto anterior, la política de “gestión de acceso de usuarios de red” debe determinar a qué información se puede acceder, los procedimientos de autorización, los controles de gestión para la protección de las redes, las conexiones de red permitidas (p. Ej., No mediante wifi), los requisitos de autenticación y la supervisión del uso.

Un proceso de control de acceso robusto pasa por los siguientes puntos realizados según la secuencia de:

**Identificación:** métodos para proporcionar un sujeto (entidad que solicita acceso) con una identidad reconocible (por ejemplo, ID usuario o cuenta de usuario, IVA, número de seguro social, pasaporte, etc.).

**Autenticación:** métodos para garantizar que un sujeto sea quien dice ser (por ejemplo, contraseña, token, huella digital, etc.). Autorización: métodos para controlar qué acciones puede realizar un sujeto en un objeto (entidad a la que se accede) (por ejemplo, lista de permisos de materia y lista de permisos de objetos).

Con respecto a los métodos de autenticación, los siguientes conceptos (o factores) se pueden usar, por separado o en combinación:

* Algo que sabe un sujeto: por ejemplo, contraseñas y PIN. Este es el menos costoso de implementar y el menos seguro.
* lgo que tiene un sujeto: por ejemplo, tarjetas inteligentes, fichas, llaves, etc. Caro, pero seguro.
* Algo que un sujeto es: por ejemplo, patrones de voz, retina, huella digital, etc. Este es el más costoso de implementar, y el más seguro.

Por lo tanto, cuando hablamos de autenticación de dos factores, nos referimos a utilizar dos de estos tres conceptos para garantizar que el sujeto sea quien dice ser.

Finalmente la norma nos proporciona los elementos a considerar en la definición de la política de acceso de usuarios a la red.

La política debe identificar:

* La red y servicios a los cuales se accede
* Los procedimientos de autorización
* Que controles tienen estos procedimientos
* Los medios por los cuales se accede (VPN, Wifi etc.)
* Los requisitos de autenticación
* Como se supervisa el uso de los servicios de red

**OBJETIVO 2 GESTIÓN DEL ACCESO DE USUARIOS**

Controles para garantizar que solamente los usuarios autorizados acceden a los sistemas y servicios

**9.2.1 REGISTRO DE USUARIOS Y CANCELACIÓN DEL REGISTRO**

Se trata de un control para el alta y baja de los usuarios

Este control exige establecer un proceso de altas y bajas que permite los derechos de acceso teniendo en cuenta:

* Un registro de IDs o cuentas de usuario donde se vincula o identifica al usuario
* Los IDs deben desactivarse automáticamente o de forma inmediata cuando el usuario abandona la organización
* Eliminación periódica de usuarios redundantes
* Los IDs redundantes nunca pueden ser asignados a otros usuarios
* El proceso de cancelación debería tener en cuenta:
  + La revocación del ID del usuario
  + La revocación de los permisos del ID de usuario

**9.2.2 GESTIÓN DE ACCESO A LOS USUARIOS**

Se debe establecer un proceso formal para asignar y revocar los accesos a sistemas y servicios que:

* Incluya la aprobación del propietario del servicio o sistema
* Verifique si el acceso cumple con las políticas de acceso definidas
* Se garantice que el acceso no se da hasta finalizar el proceso de autorización
* Se mantiene un registro de los accesos concedidos
* Se eliminan los accesos de usuarios que han abandonado la organización
* Se modifican los accesos de usuarios que han cambiado de función o puesto de trabajo si proceda
* Se revisan periódicamente los derechos de acceso

**9.2.3 GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADOS**

El control de los derechos de acceso privilegiados debe realizarse de forma independiente mediante un proceso específico que:

* Tenga en cuenta las políticas de acceso privilegiado definidas
* Se identifiquen accesos privilegiados de cada sistema o proceso
* Se tenga en cuenta las reglas generales de mínimos privilegios
* Se establezca una norma de caducidad de los permisos privilegiados
* Se definan IDs especiales o distintos para las cuentas de uso normales o no privilegiadas
* Se definan procedimientos para evitar el uso no autorizado de cuentas con derechos de acceso privilegiados
* Se verifiquen periódicamente las competencias de los usuarios
* Considerar mecanismos para mantener la confidencialidad de los datos de acceso de usuarios genéricos para los usuarios privilegiados o mecanismos para forzar el cambio de contraseñas cuando un usuario privilegiado abandona o cambia de puesto de trabajo

**9.2.4 GESTIÓN DE LA INFORMACIÓN DE AUTENTICACIÓN SECRETA DE LOS USUARIOS**

Control para garantizar que se mantiene la confidencialidad de la información secreta de acceso (p. ejemplo contraseñas).

Gestionar la información de autenticación supone controlar:

* Incluir cláusulas en contratos y condiciones de puesto de trabajo sobre el mantenimiento del secreto de las contraseñas o información de autenticación
* Obligación de cambiar contraseñas iniciales después de su primer uso
* Identificar al usuario antes de entregar las contraseñas y obtener acuse de recibo
* Uso de contraseñas seguras, no compartidas
* Uso de medios seguros de comunicación (Correos cifrados etc.)
* Cambiar contraseñas a personal externo después de que han realizado sus trabajos (instalaciones de software etc.)

Nota: donde hablamos de contraseñas como medios comúnmente utilizados para la autenticación, pero donde pone contraseñas podemos referirnos también a otros medios de autenticación como claves criptográficas, tarjetas inteligentes etc.

**9.2.5 REVISIÓN DE DERECHOS DE ACCESO DE USUARIO**

Control para establecer una revisión periódica de los permisos de accesos de los usuarios

* Revisar derechos de acceso a la terminación de empleo o cambios en la organización (cambios de empleo o promociones)
* Limitar en el tiempo los derechos de acceso con privilegios especiales
* Revisar las cuentas con privilegios especiales periódicamente y registrar los cambios que se realicen

**9.2.6 REMOCIÓN O AJUSTE DE LOS DERECHOS DE ACCESO**

Control para garantizar que se modifican los derechos de acceso al:

* Finalizar el empleo
* Cambiar de puesto de trabajo dentro de la organización

**OBJETIVO 3: RESPONSABILIDADES DEL USUARIO**

El objetivo de este control es que los usuarios sean responsables de mantener a salvo sus contraseñas o información de autenticación

Para ello se establece el siguiente control

**9.3.1 USO DE LA INFORMACIÓN DE AUTENTICACIÓN SECRETA**

Cada organización debe establecer normas para la utilización de contraseñas basando se en:

* Asegurar que las contraseñas no se divulguen
* Evitar el uso de registros de contraseñas (papel, archivos etc.)
* Políticas para cambiar las contraseñas ante amenazas
* Políticas para la calidad de las contraseñas
* Evitar el almacenamiento de contraseñas
* Forzar cambios de contraseñas iniciales
* Evitar compartir contraseñas para distintos usos

**OBJETIVO 4: CONTROL DE ACCESO AL SISTEMA Y A LAS APLICACIONES**

Se trata de prevenir accesos no autorizados a sistemas y aplicaciones con los siguientes controles:

**9.4.1 RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN.**

Las funciones de una aplicación o sistema deben considerar las restricciones de control de acceso determinadas por la política de control definido

Este sería un ejemplo de cuestiones a considerar:

CASO PRACTICO:

* Utilice menús para controlar el acceso a las distintas funciones
* Oculte las funciones de administración a los usuarios habituales
* Determine que datos son accesibles determinando que datos pueden estar disponibles para cada ID de usuario.
* Restringa de forma selectiva derechos de lectura / escritura / eliminación / ejecución etc.
* Limite el tipo de información de salida  
  Por ejemplo: Utilice gráficos que eviten el acceso a todo un archivo o carpeta
* Considere accesos físicos o lógicos adicionales para sistemas o información altamente clasificados.

**9.4.2 PROCEDIMIENTOS DE CONEXIÓN (LOG-ON) SEGUROS**

Control para establecer inicios de sesión seguros

El inicio de sesión seguro debe ser capaz de corroborar la identidad del usuario.

Cuando la clasificación de la información lo requiera por política, se debe considerar la autenticación sólida por encima y más allá de la simple identificación de usuario y contraseña. (Controles adicionales físicos o lógicos)

El procedimiento de inicio de sesión no debe mostrar los identificadores del sistema o de la aplicación hasta que el inicio de sesión haya tenido éxito.

Un centro de datos seguro no puede anunciar su nombre en el exterior del edificio. ¡Tiene que saber que está allí para encontrarlo!

Los sistemas deberían mostrar advertencias evitando proporcionar mensajes de ayuda que podrían dar pistas a los usuarios no deseados.

Los formularios de acceso deben validarse solo cuando se han completado evitando mensajes de error con información y tener algún sistema para proteger múltiples intentos de acceso mediante "fuerza bruta"

Su departamento de TI debería registrar intentos fallidos y hacer que los administradores conozcan esta información.

Después del inicio de sesión con éxito, debería mostrarse un mensaje de intentos fallidos que le permiten al usuario detectar cualquier inicio de sesión inusual.

Las contraseñas no se deben transmitir en un formato no encriptado por razones obvias. De lo contrario le estamos dando facilidades extra a los hackers.

Las sesiones inactivas deben ser dependientes del tiempo, cerradas después de un cierto tiempo o un cierto tiempo inactivo, lo que mejor se adapte a la política de la compañía.

También debe considerar si es aplicable limitar las horas del día para el acceso a las aplicaciones; no hay tantos empleados que trabajen fuera de horas, ¿debería la política de acceso reflejar este aspecto? Tenga en cuenta que, aunque sea electrónicamente, las aplicaciones son como su puerta de entrada. La información almacenada en las aplicaciones y el impacto en su pérdida o corrupción deberían guiarlo en cuanto a qué tan fuerte es esa puerta.

**9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS**

A modo de refuerzo de lo dicho hasta ahora sobre las contraseñas, los sistemas de administración deben aplicar contraseñas de calidad, rechazar contraseñas débiles, requerir confirmación y, si se emiten con ID, forzar el cambio de las contraseñas en el primer inicio de sesión.

También se deben establecer cambios de contraseñas de forma periódica, además de registrar todas las contraseñas y rechazar contraseñas similares utilizadas anteriormente. El almacenamiento de contraseñas debe mantenerse separado de los sistemas en los que se encuentran las aplicaciones.

**9.4.4 USO DE PROGRAMAS DE UTILIDAD PRIVILEGIADOS**

Aquellos programas con capacidades de anulación del sistema o sus controles deben ser restringidos y supervisados de manera especial.

Los programas con funciones privilegiadas deberían requerir autenticación por separado y estar segregados de las aplicaciones del sistema. Todas las actividades deben registrarse. Se debe considerar nuevamente la segregación de funciones cuando sea posible.

**9.4.5 CONTROL DE ACCESO AL CÓDIGO DE PROGRAMAS FUENTE**

El código fuente debe estar protegido con acceso restringido mediante el uso de librerías fuente. El código fuente no debería protegerse con aplicaciones de red.

Por otro lado se establecen controles para mantener registros de la salida y de auditoría de los cambios realizados en el código. La mayoría de las herramientas de desarrollador tienen esta función.

El desarrollo debe estar sujeto a un entorno “beta” de prueba antes del lanzamiento y la migración a la red o aplicación en operación.

**A10 CRIPTOGRAFIA**

Las medidas de control para el uso eficaz de la criptografía para proteger la confidencialidad e integridad de la información según las directrices de ISO 27001

Citando la norma:

**Objetivo 1:**  
Controles criptográficos

* **10.1.1 Política sobre el empleo de controles criptográficos**
* **10.1.2 Gestión de claves**

**OBJETIVO 1: CONTROLES CRIPTOGRÁFICOS**

**10.1.1 POLÍTICA SOBRE EL EMPLEO DE CONTROLES CRIPTOGRÁFICOS**

Los controles criptográficos están enfocados a la protección de la información en el caso de que un intruso pueda tener acceso físico a la información, se impone establecer un sistema de cifrado de la misma para dificultar la violación de su confidencialidad o su integridad

En primer lugar en una política de implementación y administración de claves de cifrado de datos se debe identificar a un responsable de la política para su implementación y administración.

La clave de la política de controles criptográficos está en identificar

* Para que información y en qué circunstancias será necesario aplicar claves criptográficas
* Los medios a emplear
* La gestión, mantenimiento y actualización de dichos medios

CASO PRACTICO:

*Dependiendo de la clasificación de la información y la evaluación del riesgo, el cifrado utilizado debe seleccionarse para que coincida en función del tipo de información, la gravedad de las amenazas y la posibilidad de que ocurran.*

*Se aconseja buscar asesoramiento especializado en esta área.*

*Comúnmente se debe considerar el cifrado para todos los tipos de medios extraíbles y aquellos que transmiten información interna y externamente. La política de encriptación debe tener en cuenta los controles utilizados para detectar / eliminar malware.*

*Los controles criptográficos se pueden utilizar como un control añadido que proporciona confidencialidad, autenticidad, no repudio y autenticación.*

**10.1.2 GESTIÓN DE CLAVES**

Los medios de cifrado implica mantener una gestión de claves criptográficas utilizadas por los medios de cifrado. La gestión de claves implica tener en cuenta políticas que tengan en cuenta el ciclo de vida completo:

* La generación
* Su uso y protección
* La distribución
* La renovación o destrucción

Como parte de la función de gestión deberemos determinar las fechas de activación y desactivación de claves en orden a reducir los riesgos mencionados anteriormente, una vez más sujetos a una evaluación de riesgos.

Cuando las claves públicas se emitan desde un proveedor externo, debe existir un “Acuerdo de nivel de servicio” para definir las responsabilidades del proveedor. Es posible que deba considerar el manejo de solicitudes legales por parte de las autoridades dependiendo de la clasificación de la información.

**A11 SEGURIDAD FISICA Y DEL ENTORNO**

En coordinación con las medidas tecnológicas ISO 27001 en este capítulo se centra en la necesidad de identificar y establecer medidas de control físicas para proteger adecuadamente los activos de información para evitar incidentes que afecten a la integridad física de la información o interferencias no deseadas

Este capítulo establece dos controles referidos a

* AREAS SEGURAS
* EQUIPAMIENTO

Citando la norma:

**Objetivo 1:**  
Áreas seguras

Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de información y la información de la organización

* **11.1.1 Perímetro de seguridad física**
* **11.1.2 Controles de acceso físico**
* **11.1.3 Seguridad de oficinas, despachos e instalaciones**
* **11.1.4 Protección contra amenazas externas y del ambiente**
* **11.1.5 El trabajo en las áreas seguras**
* **11.1.6 Áreas de entrega y de carga**

**Objetivo2:**  
Equipamiento

Prevenir pérdidas, daños, hurtos o comprometer los activos así como la interrupción de las actividades de la organización.

* **11.2.1 Ubicación y protección del equipamiento**
* **11.2.2 Elementos de soporte**
* **11.2.3 Seguridad en el cableado**
* **11.2.4 Mantenimiento del equipamiento**
* **11.2.5 Retiro de bienes**
* **11.2.6 Seguridad del equipamiento y de los activos fuera de las instalaciones**
* **11.2.7 Seguridad en la reutilización o eliminación de equipos**
* **11.2.8 Equipamiento desatendido por el usuario**
* **11.2.9 Política de escritorio y pantalla limpios**

**OBJETIVO 1: ÁREAS SEGURAS**

**11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA**

Control orientado a proveer protección contra la entrada no autorizada.

* Tanto los perímetros y controles o defensas previstas deben determinarse en un análisis o evaluación de riesgos
* **Seguridad perimetral:**  
  Los requisitos para la seguridad física deben tener en cuenta los niveles de protección del perímetro de las instalaciones o elementos que contienen la información a proteger
  + Muros
  + Vallas
  + Alarmas
  + Suelos
  + Protección de ventanas
  + Cerraduras
  + Etc.
* **Áreas atendidas:**  
  las áreas restringidas a personal autorizado deberían contar con un área de recepción atendida o medios de control adecuados para limitar el acceso físico
* **Barreras:**  
  Si es aplicable deberían considerarse barreras físicas que impidan el acceso no autorizado y protejan el área de agentes ambientales adversos
* **Sistemas Antiincendios:**  
  contar con sistemas de protección contra el fuego cumpliendo con la legislación vigente
* **Detección de intrusión:**  
  Se deben considerar sistemas de detección de intrusos (p ej. Alarmas)
* **Segmentación de espacios:**  
  Deberían separarse físicamente las áreas de proceso de información que van a ser gestionadas por personal externo de las propias de la organización

No se debe subestimar la seguridad física

Asegurar su entorno físico, y especialmente sus áreas seguras, sigue el mismo enfoque que utilizamos para proteger la información digital:

* 1. definir el contexto,
* 2. Evaluar los riesgos
* 3. Implementar los controles de seguridad más adecuados: cuanto mayor sea el valor y el riesgo, mayor será nivel de protección.
* 4. Enfrentar las amenazas ambiéntale. En seguridad física, no es suficiente con enfrentar riesgos en cuento a la seguridad sino también se necesita asegurar los equipos e instalaciones para enfrentar las amenazas ambientales VER 11.1.4 Protección contra amenazas externas y del ambiente

Veamos como cumplir estos requisitos en la práctica:

CASO PRACTICO:

*Veamos un caso práctico de cómo realizar el análisis del entorno físico para la seguridad de la información*

***Definir el contexto físico***

*En primer lugar deberíamos identificar los lugares (instalaciones y entorno), los edificios, las áreas públicas y dentro de la empresa, las áreas de trabajo y aquellas áreas seguras a proteger.*

*Los elementos a tener en cuenta en un contexto físico para poder definir cuál es la protección adecuada que necesitan son:*

***El perímetro y las fronteras***

*Aquí podemos tener en cuenta los siguientes elementos de protección:*

* 1.- El emplazamiento de la empresa (vallas o muros) o el edificio (paredes y ventanas)
* 2.- El suelo del edificio y la antigüedad del edificio
* 3.- Las estancias o divisiones dentro del edificio
* 4.- Los armarios, cajas fuertes o elementos más pequeños donde se guardan los activos de información

***Vías de acceso***

*Obviamente para la seguridad hay que tener en cuenta los medios de ingreso a las instalaciones o al entorno físico. En lo primero que pensamos es en las puertas y ventanas, pero no debemos pasa por alto los conductos de cables, las entradas y salidas de aire, etc.*

*No olvide tener en cuenta todas las formas de acceso, tanto las normales como de "emergencia" que puedan ser requeridas por las normas de seguridad.*

***Los alrededores.***

*Esto se refiere a los corredores, caminos, caminos, espacios verdes o áreas de estacionamiento que se encuentran alrededor de los perímetros.*

***Medidas de seguridad***

*Una vez identificado el entorno físico, y especialmente las áreas seguras, podemos pensar en cómo cumplir con las expectativas de seguridad para cada elemento del entorno físico.*

*Para ello deberemos definir los requisitos adecuados de protección según lo definido por un análisis y evaluación de riesgos para cada uno de los elementos del entorno físico.*

***Medidas de seguridad perimetral***

* Las medidas de protección de un recinto deben adaptarse a las necesidades de seguridad de su contenido
* Asegúrese de que las medidas de seguridad consideran el recinto en su conjunto, pues de poco sirve establecer medidas de protección muy elevadas para puertas y paredes si olvidamos los techos, suelos y ventanas
* Establezca niveles sucesivos de protección de forma que los activos más sensibles queden dentro de las áreas más seguras

***Categorización de áreas de seguridad***

*Establezca un criterio de categorías de las estancias según su contenido y organice su ubicación en relación con las demás demarcaciones de forma que pueda establecer criterios como:*

* Medidas de control de presencia y controles de acceso
* Medidas de protección volumétrica como detectores de presencia o de humo / fuego
* Medidas de control de presencia y controles de acceso
* Medidas de control de actividad
* Cámaras
* Políticas de uso de las instalaciones (Un lugar de consulta de información privilegiada no puede ser destinado al almacenamiento de equipos o de materiales)
* Medidas de control de información (no se debe dar información como carteles o indicaciones sobre la ubicación de los lugares donde se encuentra la información sensible o privilegiada)
* Medidas de control de áreas de carga, Se debe tener en cuenta que las áreas de carga nunca deben tener acceso directo a áreas seguras

***Medidas de seguridad para accesos***

*Las puertas y ventanas deben tener la misma fuerza que el perímetro: una pared fuerte y una puerta o ventana débil (o al revés, como ya se ha visto) tienen poco sentido.*

*Las normativas para el adecuado control de acceso en puertas dependen del nivel de protección necesario para la información que contienen. Siempre veneremos establecer medidas acordes de todos los elementos de seguridad de acceso a un perímetro*

* Nivel de protección de puertas y accesos (p ej. Puertas de doble acceso para prevenir entradas de personal no autorizado etc.)
* Nivel de seguridad de paredes, ventanas y suelos
* Nivel de seguridad en accesos de cables y tomas de aire
* Nivel de protección de puertas de emergencia

***Medidas de seguridad para los alrededores***

*Todos los espacios alrededor de un recinto podrían ser monitoreados (de acuerdo con el valor o la sensibilidad de la información que contienen) para prevenir, desalentar y detectar cualquier intento de ingresar (o salir) a través de puertas y otras alternativas (ventanas, conductor etc.) El monitoreo de los alrededores generalmente se realiza con cámaras o patrullas.*

**11.1.2 CONTROLES DE ACCESO FÍSICO**

Aquellas áreas que se consideran seguras deben estar protegidas por controles de entrada que permitan solo personal autorizado

* Los visitantes deben autenticarse: se debe registrar su fecha y hora de entrada / salida.
* Monitorización: La actividad debe ser monitoreada de acuerdo con la evaluación de riesgos.
* Comunicación: Se debe informar a los trabajadores que acceden sobre los procedimientos de seguridad y emergencia (especialmente en el caso de los centros de datos) y se les debe otorgar acceso para fines específicos.
* Personal Externo: Si hay personal externo autorizado y realizan el trabajo si ser acompañados por personal propio en una sala de servidores o centro de datos, debemos asegurarnos de que el acceso a otras áreas estén bloqueadas y que todo el cableado esté seguro. Se aconseja realizar una inspección física de las instalaciones al finalizar los trabajos.
* Identificaciones: Al personal que trabaje en áreas seguras se le debe exigir llevar identificación y cualquier persona que no use la identificación requerida debe ser notificada a los empleados de seguridad.
* Revisión de permisos: Los derechos de acceso deben revisarse periódicamente y revocarse según corresponda.

**11.1.3 SEGURIDAD DE OFICINAS, DESPACHOS E INSTALACIONES**

En cuanto a las instalaciones deben diseñarse para evitar al máximo posible el riesgo que la información confidencial sea accesible para los visitantes.

Se debe considerar la posibilidad de en uso de técnicas de enmascaramiento (“masking”) de datos referidos a nombres o actividades de clientes.

Supongamos por ejemplo el caso un centro de tratamiento de datos donde muchas líneas telefónicas están abiertas en cualquier momento o situaciones como la formación de usuarios o pruebas de software.

**11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y DEL AMBIENTE**

En un mundo de crecientes inestabilidades y amenazas terroristas y de un clima impredecible, se debe considerar, diseñar y aplicar la protección física contra factores externos.

Si bien las leyes vigentes nos obligan a tener planes de protección y emergencias deberíamos ir más allá y si fuera necesario buscar asesoramiento especializado.

También podríamos pensar que las amenazas externas y del medioambiente quedan cubiertos con el desarrollo de “Planes de Continuidad del Negocio” y de “Recuperación ante desastres”, sin embargo convendría considerar en este apartado las medidas de protección contra inundaciones, incendios y terremotos para mitigar sus efectos.

**11.1.5 EL TRABAJO EN LAS ÁREAS SEGURAS**

Adicionalmente a las medidas de protección física en las áreas seguras deberíamos definir procedimientos de trabajo tales como

* Prohibición de trabajos sin supervisión por parte de terceros
* Revisión de las zonas a la finalización de las visitas
* Prohibición de uso de móviles / cámaras a no ser que estén expresamente autorizados

**11.1.6 ÁREAS DE ENTREGA Y DE CARGA**

Los puntos de carga suelen ser puntos sensibles para la seguridad física por lo que deberíamos tomar en cuenta algunos aspectos de control en nuestra evaluación de riesgos tales como:

* Horarios definidos de apertura y cierre
* Control de apertura y cierre de puertas externas e internas
* Control de personal
* Realización de inventarios de materiales entregados
* Revisión de mercancías entregadas para detectar materiales peligrosos
* Separar entregas entrantes y salientes
* Necesidad de informar de cualquier incidente a los responsables de seguridad
* Barreras adicionales de seguridad

**OBJETIVO2: SEGURIDAD DE LOS EQUIPOS**

Los daños en los equipos pueden causar interrupciones en la actividad de una organización o vulnerar la confidencialidad de la información causada por robos de activos

Veamos los controles que deberemos revisar en nuestra evaluación de riesgos para la seguridad de la información

**11.2.1 UBICACIÓN Y PROTECCIÓN DEL EQUIPAMIENTO**

Controles para proteger los equipos de daños ambientales y accesos no autorizados

* Evitar accesos no necesarios
* Proteger los equipos de áreas sensibles como centros de datos o salas de servidores
* Controles de protección en lugares de almacenamiento de equipos si estos contienen información
* Medidas de protección contra daños eléctricos (fuentes de alimentación reguladas, líneas de alimentación separadas y respaldadas etc.)
* Control medioambiental para cumplir con las especificaciones del fabricante en cuanto a condiciones de humedad, temperatura protección contra polvo o materiales que puedan dañar los equipos
* Medidas de protección contra radiaciones
* Deben establecerse pautas para comer, beber y fumar cerca del equipo para evitar daños o simplemente evitar que los empleados estén en contacto con los equipos si no están trabajando en ellos.

**11.2.2 ELEMENTOS DE SOPORTE**

Se trata de establecer medidas de control para el suministro necesario para mantener operativas las instalaciones y los equipos

A menudo este capítulo se pasa por alto en pequeñas y medianas empresas pero conviene que tengamos en cuenta controles para garantizarnos según nuestras posibilidades la cobertura ante fallos del suministro eléctrico y las comunicaciones.

Los controles de este apartado van enfocados a:

* Cumplir con las especificaciones del fabricante de los equipos en cuanto a suministros (electica, gas etc.)
* Cumplir los requisitos legales
* Establecer algún proceso de detección de fallos de suministro
* Mantener si es posibles alternativas a fallos de suministro (sistemas de alimentación ininterrumpida, rutas alternativas en comunicaciones etc.)

En este apartado deberemos ser imaginativos pues no siempre está a nuestro alcance poder duplicar las comunicaciones o los suministros de energía eléctrica o gas etc. A veces pasa por reforzar sistemas como Teletrabajo, soportes CLOUD o convenios con empresas más grandes como clientes importantes de confianza con mayor infraestructura en caso de desastres que no podamos asumir.

**11.2.3 SEGURIDAD EN EL CABLEADO**

Controles para protección del cableado de energía y de comunicaciones que afecta a los sistemas de información

Se trata de evitar tanto el posible daño de las infraestructuras como las posibles interferencias que corrompan los datos o el suministro

**RECOMENDACIONES**

Los cables deben estar bajo tierra hasta el punto de acceso dentro de la instalación, de o alternativamente debería pensarse en otro tipo de protección.

Los cables de potencia deben estar separados de los cables de comunicaciones para evitar interferencias.

Los puntos de acceso del cableado a los equipos o a las salas deben asegurarse según corresponda y los cables deben estar protegidos.

Como medidas adicionales podríamos realizar barridos técnicos de los cables de comunicación para dispositivos no autorizados (bugs y sniffers) conectados al cableado.

El cableado alrededor de las salas de servidores y centros de datos debería estar aislado de forma segura para evitar la conexión de dispositivos no autorizados.

Finalmente deberemos tener en cuenta siempre el acceso restringido y controlado a las sales de paneles de conexión

**11.2.4 MANTENIMIENTO DEL EQUIPAMIENTO**

Se trata de controles para garantizar que los equipos se mantienen adecuadamente para garantizar que no se deterioren y estén siempre disponibles.

Para ello deberíamos tener en cuenta

* Las recomendaciones del fabricante
* Solo personal autorizado debe mantener equipos críticos y se deben mantener registros.
* La información sensible debería removerse del equipo cuando sea necesario
* Cumplir con todos los requisitos de las pólizas de seguros

**11.2.5 RETIRO DE BIENES**

Cuando se trata de la retirada de un activo de información ya sea equipos, software u otros dispositivos de información deberíamos controlar

* La identificación y autorización de personal autorizado a retirar equipos o activos fuera de la organización
* Fijar límites de tiempo
* Llevar un registro de equipos retirados y de su retorno así como de la identificación de personal.

**11.2.6 SEGURIDAD DEL EQUIPAMIENTO Y DE LOS ACTIVOS FUERA DE LAS INSTALACIONES**

Mantenga un registro de la custodia de los activos que abandonan la organización y realice evaluaciones de riesgo para instalaciones donde serán utilizados

**11.2.7 SEGURIDAD EN LA REUTILIZACIÓN O ELIMINACIÓN DE EQUIPOS**

Para los equipos que van a ser reutilizados deberíamos garantizar

* La información que contenían se ha destruido o sobre escribido correctamente antes de su reutilización
* Garantizar que las información se ha eliminado completamente considerando que los formateos estándar no realizan esta tarea de forma adecuada
* Los equipos averiados deben estar sujetos a una evaluación de riesgos antes de disponer de ellos para una reparación

**11.2.8 EQUIPAMIENTO DESATENDIDO POR EL USUARIO**

Los usuarios no deben dejar las sesiones abiertas mientras el equipo no este atendido.

Además de los procedimientos de bloqueo de pantalla, la sesión de la aplicación y de la red debe cerrarse cuando las conexiones no se utilizan.

Esto debería aplicarse tanto a los dispositivos móviles como a los equipos fijos.

**11.2.9 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS**

Una de las políticas de seguridad más fácilmente reconocidas y que más se incumple en la práctica y que podríamos decir que se aplica a todas las personas en todas las organizaciones.

Las pantallas no deben mostrar información cuando el equipo no esté en uso y los escritorios deben estar libres de papeles cuando no estén en uso o desatendidos.

Dependiendo de la clasificación de los documentos en papel y la cultura de la organización, el papel y los medios extraíbles deben asegurarse según la política cuando no estén en uso.

Las evaluaciones de riesgos deberían considerar el uso de tecnologías que permitan realizar copias de la información tales como: Impresoras, fotocopiadoras, escáneres y cámaras (especialmente en teléfonos)

Las impresoras se pueden configurar de modo que solo el creador pueda acceder a las copias una vez que se haya ingresado un código en la máquina para evitar el acceso no autorizado.

**A12 SEGURIDAD DE LAS OPERACIONES**

Entramos en un capitulo de ISO 27001 con una serie de controles con un fuerte componente técnico.

No olvidemos que una buena utilización de esta guía debe tener en cuenta la aplicación práctica de estas recomendaciones y controles seleccionando aquellos aspectos que puedan aportar un mayor beneficio a la organización siempre bajo el criterio del análisis de riesgos para la seguridad de la información.

Citando la norma:

**Objetivo 1:**  
Procedimientos operacionales y responsabilidades

Se trata de asegurar la operación correcta y segura de las instalaciones de procesamiento de información.

* **12.1.1 Procedimientos documentados de operación**
* **12.1.2 Gestión de cambios**
* **12.1.3 Gestión de la capacidad**
* **12.1.4 Separación de los ambientes para desarrollo, prueba y operación**

**Objetivo2:**  
Protección ante software malicioso

Garantizar que la información y las instalaciones de procesamiento de información se encuentren protegidos contra el código malicioso..

* **12.2.1 Controles ante software malicioso**

**Objetivo 3:**  
Respaldo

Registrar eventos y generar evidencia

* **12.3.1 Respaldo de la información**

**Objetivo 4**  
Registros y supervisión

* **12.4.1 Registro de eventos**
* **12.4.2 Protección de la información de registros (logs)**
* **12.4.3 Registros del administrador y operador**
* **12.4.4 Sincronización de relojes**

**Objetivo 5:**  
Control de software en la producción

Garantizar la integridad de los sistemas operativos

* **12.5.1 Instalación de software en los sistemas operativos**

**Objetivo 6:**  
Gestión de vulnerabilidad técnica

Prevenir la explotación de vulnerabilidades técnicas

* **12.6.1 Gestión de vulnerabilidades técnicas**
* **12.6.2 Restricciones en la instalación de software**

**Objetivo 7:**  
Consideraciones sobre la auditoría de sistemas de información

Minimizar el impacto de las actividades de auditoría en los sistemas operativos

* **12.7.1 Controles de auditoría de sistemas de información**

**OBJETIVO 1: PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES**

**12.1.1 PROCEDIMIENTOS DOCUMENTADOS DE OPERACIÓN**

Los procedimientos deben estar documentados (cuando corresponda) y estar disponibles.

Vamos por partes:

***¿Qué debemos documentar?***

La documentación de procedimientos al menos debería abarcar aquellas actividades que afectarán al procesamiento de la información y aquellas que la protegen.

Siguiendo este principio deberíamos incluir

* Los procesos de verificación, instalación, configuración y administración de sistemas y aplicaciones;
* El procesamiento y manejo de la información;
* Los procesos de gestión de respaldo de la información, incluidas las pruebas y la verificación de copias de seguridad;
* La gestión de la programación operacional en el caso de procesos que requieran programación de tiempos
* De acuerdo con los requisitos de la norma ISO 27001 también deberíamos incluir el manejo de errores y condiciones excepcionales que pueden definirse como incidentes de seguridad.
* Instrucciones especiales de manejo de medios para información confidencial, incluida la eliminación segura. Recuperación / reinicio del sistema.
* Los procesos de gestión de registros y elementos de seguimiento de auditoría.
* Los procedimientos de monitoreo de red y activos de información.

***¿Qué significa que estén disponibles?***

Esto se traduce en que deberíamos realizar actividades de formación y concienciación sobre los procedimientos sobre el tratamiento de la información y su cuidado o seguridad

**12.1.2 GESTIÓN DE CAMBIOS**

Los procesos de cambio pueden conllevar riesgos asociados para la seguridad de la información. Es por ello que la norma nos propone controles para que analicemos los procesos de cambio tanto:

* Comerciales
* Instalaciones o infraestructuras (Equipos y Software)
* Sistemas de procesamiento de información

A estas alturas resulta obvio decir que los controles a establecer para la gestión de cambios serán el resultado del análisis de riesgos y de la aplicabilidad de los controles proporcionados por este anexo.

En resumen podríamos decir que:

Las evaluaciones de riesgos deberían exigir siempre una autorización formal para la realización de cambios.

Otro elemento esencial es establecer siempre una planificación para los cambios a realizar en equipos, sistemas software etc. Acompañado de pruebas realizadas y comunicaciones a todos los involucrados.

Finalmente, deberíamos mantener un registro que contenga al menos la información de:

* Quien autoriza los cambios
* Quien realiza los cambios
* Fecha
* Descripción de las tareas
* Validación del cambio
* Otros

Esta información será útil en una auditoría para proporcionar la confianza de que los cambios se han realizado de forma controlada.

**12.1.3 GESTIÓN DE LA CAPACIDAD**

Se trata de evitar pérdidas de disponibilidad o rendimiento de los sistemas por falta de capacidad.

Gestionar la capacidad se refiere a tener un control del uso de los recursos. Esto se traduce en controles para:

* Medición y Seguimiento del uso de recursos
* Previsión de uso a futuro (prever “cuellos de botella”)
* Planificar las ampliaciones de capacidad de los recursos cuando sea necesario
* Optimizar el uso de recursos. P ej. Considere la posibilidad de optimizar las consultas a sus bases de datos, realizar procesos por lotes fuera de horas de carga de trabajo, eliminación de archivos de datos antiguos y aceleración del ancho de banda para accesos no críticos.

**12.1.4 SEPARACIÓN DE LOS AMBIENTES PARA DESARROLLO, PRUEBA Y OPERACIÓN**

Este punto nos pone como requisito separar los entornos de desarrollo de los entornos de producción para evitar problemas de indisponibilidad o fallos en el servicio.

Los entornos de desarrollo, código fuente y herramientas de desarrollo, tampoco deberían estar disponibles para los entornos de producción para evitar problemas de seguridad

En cuanto a los datos que se utilizan en entornos de desarrollo no deberían ser una copia de los datos de producción a menos que se hayan previsto controles de seguridad (acuerdos de confidencialidad etc.) similares a los entornos de desarrollo.

Tengamos en cuenta que un desarrollador se encuentra en una posición privilegiada para introducir código malicioso o simplemente código no probado, y ante esto deberíamos tener controles para evitarlo.

Se debe prestar especial atención a la migración del código al entorno operativo con las “pruebas beta” planificadas y la disponibilidad de entornos estables conocidos disponibles por si se encuentran errores.

**OBJETIVO2: PROTECCIÓN ANTE SOFTWARE MALICIOSO**

Garantizar que la información y las instalaciones de procesamiento de información se encuentren protegidos contra el código malicioso...

**12.2.1 CONTROLES ANTE SOFTWARE MALICIOSO**

El creciente problema de los ataques contra la seguridad de la información hace que estos controles sean de lo más aplicables y prácticos para cualquier organización.

En primer lugar deberemos disponer de sistemas de detección de código malicioso en los servidores y en los puestos de trabajo.

**Requisitos para los Usuarios**

La primera línea de defensa para evitar la entrada de código malicioso son los propios usuarios deben estar preparados para saber responder ante posibles incidencias detectadas.

En primer lugar será necesario establecer un procedimiento de seguridad dirigido a los usuarios para que conozcan sus obligaciones respecto a la seguridad de la información y evitemos que abran archivos adjuntos sin asegurarse de que no sean maliciosos, no hagan clic en enlaces en correos electrónicos ni visiten sitios web que puedan cargar virus, troyanos o rastreadores en el dispositivo del usuario etc.

Considere poner en la lista negra sitios conocidos o restringir el uso de internet en los puestos de trabajo si no es necesario para el desempeño de sus funciones.

**Requisitos para los Sistemas**

La segunda línea de defensa debe enfocarse al acceso a los sistemas para restringir cómo los usuarios conectan medios extraíbles u otros dispositivos a las redes para evitar la introducción de material no verificado.

CASO PRACTICO:

*Un dispositivo USB ha estado en muchos lugares podría introducir cualquier cosa aún en sus redes con muchas barreras de seguridad.*

*Las encuestas nos revelan que la mayoría de los usuarios conectarían un USB que simplemente habían encontrado en cualquier lugar.*

*Es por ello que debemos tomar medidas tanto de protección como de prevención para este tipo de comportamientos. En este caso la formación de una cultura de la seguridad en las empresas es fundamental*

Las medidas de protección para la red son muy útiles, tales como programas antivirus que controlen los archivos que se procesan o envían por correo electrónico.

La desactivación de macros antes de descargar archivos puede ser una ayuda muy eficaz en la lucha contra el malware

Se debe establecer una política para prohibir la introducción de software no autorizado y proteger contra archivos o software de fuentes externas.

Algunos requisitos para abordar la detección de Software malicioso

* Definir responsabilidades sobre los que tienen la misión específica de realizar las tareas detección de malware y las de los usuarios
* Realizar las capacitaciones necesarias para que el personal dedicado a la tarea de detección de Software malicioso tenga los conocimientos necesarios
* Capacitar a los usuarios para que sepan cómo deben actuar cuando reciben una alarma de detección de software malicioso
* Establecer procedimientos para las tareas de mantenimiento y las situaciones de emergencia
* Establecer procedimientos de aislamiento en caso de detección y recuperación de cualquier ataque.
* Incluir en las políticas de seguridad las acciones y procedimientos establecidos en los planes de continuidad del negocio para casos de recuperación ante incidentes

Otros criterios para las políticas de detección de Malware

* Establecer sistemas de monitoreo de software y los datos de la red.
* La localización de archivos o parcheo software no aprobados deben investigarse y resolverse como incidentes de seguridad.
* Los equipos deberían escanearse periódicamente especialmente cuando se va a instalar un nuevo software
* Los escaneos deberían incluir archivos adjuntos de correo electrónico, descargas y páginas web.
* La formación continúa a los empleados como herramienta para mantener actualizados a los usuarios de las nuevas amenazas y de cómo responder a ellas.
* Los empleados deben conocer también cuales son los problemas que puede causar el software malicioso.

**OBJETIVO 3 RESPALDO - COPIAS DE SEGURIDAD**

Evitar la pérdida de datos mediante la aplicación de una política de copias de seguridad que permita asegurar la disponibilidad e integridad de la información ante incidentes.

Este objetivo incluye un único control:

**12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACIÓN**

El proceso de copias de seguridad de la información debería ser definido por una política de copias de seguridad o de respaldo de la información que tenga en cuenta la periodicidad con la que se hacen las copias, esto dependerá de las necesidades de recuperación de cada tipo de información

Otros aspectos a tener en cuenta serian

Alcance de las copias de seguridad

Asegúrese que las copias de seguridad tienen un alcance que cubra todas las necesidades de respaldo de su información:

* Datos e información sensible
* Software y aplicaciones
* Datos de configuración de aplicaciones Sistemas etc.
* Datos sobre accesos, claves etc.
* Registros de actividades, eventos, mensajes o alarmas del sistema

**Verifique su validez**

Comprobar que las copias son válidas es una actividad que no se realiza normalmente en empresas pequeñas y medianas, sin embargo puede resultar embarazoso comprobar después de un desastre que los archivos de copia de seguridad no se restauran convenientemente, por lo que resulta de lo más tranquilizador el realizar una verificación de la validez de las copias de seguridad mediante algún proceso de restauración simulado o en algún equipo de prueba

**Ubicaciones Alternativas**

No solo es importante realizar las copias de seguridad sino la ubicación donde se encuentran. Es muy aconsejable establecer ubicaciones alternativas al emplazamiento de los datos o aplicaciones para aumentar la seguridad ante posibles impactos de desastres ambientales, accidentes, incendios etc.

**Medios de recuperación**

Los medios de recuperación son tan importantes como las propias copias de seguridad por lo que deberemos tener en cuenta el mantenimiento en perfecto estado de funcionamiento de los medios que nos permitirán la restauración de las copias cuando las necesitemos

**Restauraciones parciales**

Los medios de recuperación y el sistema de copias de seguridad deberían permitir restauraciones parciales del sistema dependiendo de las distintas aplicaciones y sistemas de forma que un incidente de corrupción de un sistema o aplicación no obligue a la restauración de otras aplicaciones con el consiguiente impacto.

**Mantener registros**

Mantenga registros de las copias de seguridad como parte de un cronograma o plan de mantenimiento de copias de seguridad. También es aconsejable mantener un registro de las pruebas de validez de dichas copias.

**Nivel de protección**

Mantenga el mismo nivel de protección para las copias de seguridad que los requeridos para los datos operativos y cuando sea necesario las copias de seguridad deben estar encriptadas

Finalmente, los planes de continuidad del negocio deben tener en cuenta el tiempo requerido para realizar restauraciones completas del sistema, lo que puede requerir una operación diversa en varios sitios.

**OBJETIVO 4 REGISTROS Y SUPERVISIÓN**

Cuando todo marcha bien este punto quizás no tenga mucha utilidad, sin embargo ante un incidente en la seguridad de la información, resulta un punto indispensable ya que sino no sabríamos por dónde empezar a investigar. Esta es la principal razón por la que los sistemas de información deben mantener registros que a su vez deben ser monitoreados.

Estamos hablando de trazabilidad de los eventos. Para este objetivo, deben definirse las necesidades de trazabilidad o monitorización de cada sistema de información. De esta forma, podremos aplicar un sistema de registros que nos permitan identificar la autoría y los tipos de las acciones que se han ejecutado en dicho sistema.

Los registros que se determinan como controles sobre los sistemas de información son:

**12.4.1 REGISTRO DE EVENTOS**

En primer lugar parece obvio que deberemos mantener un registro de los eventos pues a la hora de un incidente querremos determinar qué estaba sucediendo mediante los datos de la hora, la fecha del incidente, etc., las personas involucradas, el origen y las causas, etc.

La primera tarea será determinar los distintos eventos a registrar en cada sistema:

* Intentos de acceso exitosos y fallidos,
* Desconexiones del sistema
* Acciones ejecutadas,
* Alertas por fallos en el sistema
* Fecha y hora en que se producen los eventos
* Tiempos de detención
* Etc.

**ASPECTOS LEGALES**

Tener un sistema sin un registro de eventos puede ser un grave error ya que en algunos casos puede implicar sanciones por incumplimiento de las normas legales sobre protección de datos personales.

**PREVENIR INCIDENTES**

Revisar los registros de forma periódica, independientemente de si hay un incidente o no puede ayudarnos a analizar tendencias, detectar potenciales actividades fraudulentas, o detectar el origen de fallos de funcionamiento, antes de que ocurran incidentes importantes.

**12.4.2 PROTECCIÓN DE LA INFORMACIÓN DE REGISTROS (LOGS)**

Los registros de eventos deben tener el nivel de protección apropiado para evitar pérdidas, corrupción o cambios no autorizados.

Donde sea posible, el administrador del sistema no debe tener permiso para borrar o desactivar el registro de sus propias actividades.

También se deberían guardar copias de seguridad de los registros de eventos

La detección de intrusiones debería ser administrada fuera del alcance de los administradores de red para cumplir con este requisito

**12.4.3 REGISTROS DEL ADMINISTRADOR Y OPERADOR**

Como ya hemos adelantado en el punto anterior, deberemos registrar las actividades no solo de los usuarios sino también de los administradores, teniendo especial cuidado con los que tienen privilegios de administración dado el riesgo que tiene si pueden acceder a los registros y manipularlos o borrarlos.

**12.4.4 SINCRONIZACIÓN DE RELOJES**

Aunque existan otros requisitos de sincronización en el sistema, a la hora de registrar eventos es imprescindible que todos los sistemas de procesamiento estén sincronizados. Para cumplir con este requisito, el proceso de sincronización debe estar documentado con los requisitos necesarios para que esto se cumpla.

**OBJETIVO 5 CONTROL DE SOFTWARE EN LA PRODUCCIÓN**

Desgraciadamente todos tenemos experiencias de incompatibilidades en instalaciones de nuevo software o en actualizaciones de versiones existentes. Esto puede afectar tanto al funcionamiento del propio software o aplicación como al rendimiento de los equipos y afectar de rebote a otros sistemas o aplicaciones

Para evitar estos problemas se establece el siguiente control:

**12.5.1 INSTALACIÓN DE SOFTWARE EN LOS SISTEMAS OPERATIVOS**

Es importante mantener procedimientos para cubrir las instalaciones de Software en cualquier dispositivo dentro de una organización. Estos procedimientos deben fijarse en la aplicabilidad de los siguientes controles

* Probar las nuevas aplicaciones o software en entornos aislados especialmente preparados para pruebas
* Comprobar las necesidades de instalación (compatibilidad del entorno) antes de su instalación
* Valorar la necesidad de actualización o instalación
* Planificar la forma de volver a versiones anteriores en caso de ser necesario
* Los entornos de desarrollo deben permanecer aislados de los entornos operativos
* Las instalaciones de software debe ser realizada por usuarios autorizados
* Establecer procedimientos o herramientas de monitoreo del software para detectar cambios no autorizados
* Las pruebas posteriores a la implementación deben incluir una supervisión de la red para identificar cualquier tráfico inesperado que pueda exponer errores o suponga empeoramiento de la velocidad de las transmisiones.

**OBJETIVO 6 GESTIÓN DE VULNERABILIDAD TÉCNICA**

Actualmente todas las aplicaciones software están sujetas a actualizaciones con propósito de mejorar no solo su funcionalidad sino sobre todo la seguridad de las mismas

Este apartado nos indica controles para evitar que las posibles vulnerabilidades del software puedan ser aprovechadas por los atacantes

**12.6.1 GESTIÓN DE VULNERABILIDADES TÉCNICAS**

Ante lo expuesto anteriormente queda claro que no sirve quedarnos de brazos cruzados ante un entorno cada vez más hostil en el mundo de las aplicaciones software.

Es por ello que debemos gestionar nuestras posibles vulnerabilidades identificando nuestras posibles debilidades técnicas mediante

* La consulta de foros especializados
* Mantener actualizada la información de fabricantes y proveedores
* Realizar pruebas de ataques simulados (hacking ético)
* Escaneos periódicos de vulnerabilidades

*Algunos consejos prácticos*

*Un buen punto de partida para realizar un buen análisis de vulnerabilidades técnicas es tener en cuenta el registro de activos de información.*

*El inventario de activos de información convenientemente documentado debería ser su guía para evaluar e implementar controles para abordar la vulnerabilidad técnica.*

*Aquí es donde aplicamos los criterios de cómo están siendo monitoreados los activos de información, cuál es su evaluación de riesgos y los controles que deberemos aplicar para abordar nuestras vulnerabilidades técnicas.*

*Administrar convenientemente nuestros activos de información puede traernos muchos beneficios ya que nos permite tener la herramienta de decisión para abordar temas como:*

* *Como puedo reducir el número de aplicaciones software*
* *Qué tipo de aplicaciones cumplen con las reglas y objetivos de la seguridad de la información y están alineadas con los objetivos del negocio y así identificar y trabajar para eliminar aquellas que no las cumplen*
* *Establecer entornos de datos cada vez más confiables para reducir en la manera de lo posible las actualizaciones y parcheo del software*

*En segundo lugar el monitoreo de los sistemas es la herramienta que nos puede brindar valiosa información para tomar decisiones en cuanto a la identificación de vulnerabilidades técnicas*

*Lo que no se monitorea se desconoce, así que establezca registros y mediaciones (KPI) de los efectos de las actualizaciones de software incluyendo por ejemplo:*

* *Cronogramas efectivos para realizar las notificaciones*
* *Elementos de medición en aplicaciones no tan comunes como software de control, dispositivos de los empleados, móviles etc.*
* *Evalué la eficacia de las actualizaciones antes de generalizarlas a toda la organización mediante sistemas piloto o pruebas en pequeña escala*

*En tercer lugar establezca una política de control para la instalación de software (esto lo veremos en el siguiente punto)*

**12.6.2 RESTRICCIONES EN LA INSTALACIÓN DE SOFTWARE**

Aunque ya se menciona en puntos anteriores la norma quiere insistir en establecer restricciones para la instalación de software por parte de los usuarios.

Ya quedo claro que la instalación de software debe realizarse por personal autorizado y con la capacitación adecuada. Aquí se trata de que además definamos unas reglas concisas para limitar la capacidad de los usuarios finales.

Estas restricciones deben ir enfocadas a identificar expresamente:

* Qué tipos de instalaciones de software son las permitidas a los usuarios finales (por ejemplo, actualizaciones y parches de seguridad al software existente)
* Qué tipos de instalaciones se encuentran prohibidas (por ejemplo, software que es sólo para uso personal y software cuyo origen pueda ser potencialmente dañino etc.

**OBJETIVO 7 CONSIDERACIONES SOBRE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN**

Minimizar el impacto de las actividades de auditoría en los sistemas operativos

Algunas auditorias sobre sistemas de información pueden conllevar una intención con los dichos sistemas. Se trata de establecer controles para minimizar este impacto mediante la planificación de actividades de forma que causen la mínima interferencia en sistemas operativos.

**12.7.1 CONTROLES DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN**

Se trata de auditorías técnicas sobre sistemas, No se refiera este punto a la auditoria de cumplimiento de la norma ISO 27001 sino más bien a las auditorias de los sistemas de información para evaluar cosas como:

* ¿Los usuarios están trabajando con los privilegios correctos?
* ¿La infraestructura es estable y confiable?
* ¿Las infraestructuras cuentan con la suficiente capacidad (memoria, procesamiento, almacenamiento, ancho de banda)?
* ¿Cómo puede ser mejorado?
* ¿Las pruebas realizadas son efectivas?
* ¿Cuán efectivas son las actividades de mantenimiento, monitoreo y gestión?
* ¿Qué hacen los usuarios del sistema?

En este aspecto deberemos controlar que las auditorias para obtener esta información

**1 Cumplan con el alcance planificado.**

En la práctica el alcance de las auditorias puede ser demasiado abierto de forma que la auditoría podría convertirse en una enorme tarea que reduce su propio valor, perdiendo un enorme esfuerzo en cosas que son de poca importancia. Delimitar las auditorias es una primera y primordial tarea para no devaluar su significado y para que realmente sean útiles

**2 Evaluar y considerar el impacto**

Se debe evaluar el impacto o consumo de recursos de auditorías que supongan un consumo de recursos importante dentro de los sistemas. En este caso debe existir un procedimiento por el cual se evite realizar estas tareas que pueden comprometer la capacidad de los sistemas realizándolas en periodos de baja carga de trabajo

**A13 SEGURIDAD EN LAS COMUNICACIONES**

Hoy en día la información viaja por la red de comunicaciones de cualquier empresa u organización por más pequeña que sea. Quien ya no transmite información aunque sea solo por email o por whatsapp?

Puesto que los intercambios de información se realizan a través de redes de comunicaciones deberemos establecer los controles adecuados para proteger tanto las comunicaciones externas a la organización como las que viajan a través de las redes de la propia organización

Citando la norma **ISO 27001**:

**Objetivo 1:**  
Gestión de la seguridad de red

Asegurar la protección de la información en redes y la protección de la infraestructura de soporte

* **13.1.1 Controles de Red**
* **13.1.2 Seguridad de los servicios de red**
* **13.1.3 Separación en redes**

**Objetivo 2:**  
Intercambio de información

Mantener la seguridad de la información intercambiada dentro de una organización y con cualquier otra entidad.

* **13.2.1 Políticas y procedimientos de intercambio de información**
* **13.2.2 Acuerdos de intercambio de información**
* **13.2.3 Mensajería electrónica**
* **13.2.4 Acuerdos de confidencialidad y de no divulgación**

**OBJETIVO 1: GESTIÓN DE LA SEGURIDAD DE RED**

La estructura típica de la gran mayoría de organizaciones cuenta con una red interna que interconecta los distintos dispositivos y sistemas además de ocuparse de realizar las comunicaciones con el exterior. Veamos los controles previstos para todos los elementos posibles de una red de comunicaciones:

**13.1.1 CONTROLES DE RED**

Para gestionar una red asegúrese de que se han asignado responsabilidades dentro del equipo de gestión y que se siguen una serie de procedimientos establecidos.

Considere la posibilidad de separar el control de la red de las tareas de operación.

Los principales elementos a gestionar dentro de una red son los elementos físicos que dan soporte a la red y sobre todo los que nos interconectan con el exterior (routers, switch, etc.). Además de los elementos físicos, también considere como elementos a controlar las transmisiones de datos.

Cuando la información se transfiere a través de redes públicas o redes inalámbricas, se deben considerar controles adicionales para mantener las conexiones (disponibilidad) y la privacidad (confidencialidad) y la integridad de los datos.

**MONITOREO Y REGISTRO**

El monitoreo y registro de las actividades en la red debemos utilizarlo tanto para establecer medidas correctivas y si es necesario disciplinarias como para establecer medidas preventivas. Si podemos corregir algo mediante un programa de concienciación siempre será mejor que tomar acciones disciplinarias.

**CONTROL DE ACCESO**

Si es posible, la autenticación de inicio de sesión para el uso de la red puede ser implementada mediante un sistema de garantía de factores múltiples.

Hoy en día los accesos con ID de huella digital o mediante el uso adicional del teléfono móvil podemos aumentar la seguridad de las simples contraseñas permitiéndonos evitar accesos no autorizados aunque se conozca la contraseña.

**CONTROL DE PRIVILEGIOS**

Como control fundamental de cualquier sistema las conexiones de red también deben estar restringidas según los privilegios asignados.

**13.1.2 SEGURIDAD DE LOS SERVICIOS DE RED**

Independientemente de si los servicios de red son internos o externos (subcontratados), deberían definirse requisitos en relación a la calidad de servicio mediante acuerdos de Niveles de Servicio o SLA. Las auditorias de la calidad de servicios prestados es el único modo en que podemos tener visibilidad sobre la disponibilidad de la red y evaluar los riesgos a los que estamos expuestos con dichos servicios ya que de ellos depende la operatividad de los sistemas de información

**13.1.3 SEPARACIÓN EN REDES**

Además del acceso restringido a la red, la subdivisión de las redes en distintos dominios permite una mayor seguridad. En esto consiste la segregación o separación de redes que puede aplicarse de forma lógica o incluso física.

*Algunos consejos prácticos*

*Algunas organizaciones tienen información altamente clasificada en dispositivos que están físicamente protegidos y no están conectados a redes en absoluto, por lo que la información solo se procesa en un entorno sin conexión a red.*

*Aquí es donde aplicamos los criterios de cómo están siendo monitoreados los activos de información, cuál es su evaluación de riesgos y los controles que deberemos aplicar para abordar nuestras vulnerabilidades técnicas.*

*Las redes inalámbricas son particularmente vulnerables con respecto a la seguridad y esto debe considerarse como parte de la estrategia de segregación.*

**OBJETIVO2 INTERCAMBIO DE INFORMACIÓN**

Se trata de requisitos o controles para proteger la información cuando se transmiten datos bien sea internamente o entre varias entidades

**13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACIÓN**

Defina procedimientos y políticas para proteger la información que se va a transmitir donde se tenga en cuenta todos los aspectos.

* Los medios de transmisión
* Las redes
* Los soportes informáticos
* Los soportes documentales
* Etc.

Las medidas de seguridad deberán definirse en función de la naturaleza del remitente, el destinatario y los soportes utilizados.

Tenga en cuenta que la transferencia de datos puede estar sujeta a requisitos legales.

Las políticas y los procedimientos deben incluir requisitos para la protección contra intercepción, copia, modificación, dirección incorrecta o destrucción. Esto debe estar respaldado por políticas de uso aceptable, una política que cubra el manejo de archivos adjuntos, el uso de encriptación y cualquier seudonimización de datos (ver GDPR).

**13.2.2 ACUERDOS DE INTERCAMBIO DE INFORMACIÓN**

Deben existir acuerdos entre las partes de intercambio de información para garantizar tanto el uso que se le va a dar a la información como los niveles de protección. Estos acuerdos deberían tratar puntos tales como:

* La responsabilidad de las partes en el uso y protección y custodia de la información
* La trazabilidad de los datos
* El cumplimiento de las normas técnicas y legales
* Los requisitos de cifrado
* Las responsabilidades en la cadena de custodia
* Los controles de acceso a la información

**13.2.3 MENSAJERÍA ELECTRÓNICA**

El correo electrónico debe ser tratado como un activo más de información donde se apliquen controles apropiados para mantener la confidencialidad, Integridad y disponibilidad de la información.

Dentro de la mensajería electrónica también deberemos incluir los mensajes de chat electrónico así como redes sociales.

Los controles aplicables a la mensajería electrónica serian:

* Protección ante acceso no autorizado (mensajes encriptados etc.)
* Asegurar el correcto direccionamiento y transporte de los mensajes;
* Confiabilidad y disponibilidad del servicio
* Consideraciones legales (firmas digitales)
* Necesidad de autorización para usar servicios públicos externos (mensajería instantánea, redes sociales y compartir archivos)
* Medidas adicionales de autenticación en accesos desde redes públicas

**13.2.4 ACUERDOS DE CONFIDENCIALIDAD Y DE NO DIVULGACIÓN**

Los acuerdos de confidencialidad afectan tanto a la información propia de la empresa como a informaciones que provengan de terceras partes por lo que deberíamos considerar acuerdos de confidencialidad tanto a personal propio como a clientes y proveedores si tiene acceso a activos de información que así lo requieran.

Los acuerdos de confidencialidad y de deber de secreto hay que tenerlos firmados por escrito antes de iniciar una transferencia de información.

Los acuerdos deben cubrir:

* La naturaleza de la información
* La duración del acuerdo
* Los procedimientos de rescisión
* Las responsabilidades y las propiedades,
* El uso permitido de la información
* El derecho de auditoría
* Los procesos a llevar a cabo en caso de una infracción
* Cláusulas que obliguen a mantener el deber de secreto debe incluso más allá de la relación profesional entre las dos entidades.

**A14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**

El objeto de este apartado es la aplicación controles para la seguridad de la información al ciclo de vida completo de los sistemas de información, tanto propios como subcontratados

Citando la norma **ISO 27001**:

**Objetivo 1:** Requisitos de seguridad de los Sistemas de información

Garantizar que la seguridad de la información es una parte integral de los sistemas de información en todo su ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan servicios través de. Redes públicas.

* **14.1.1 Análisis y especificación de los requisitos de seguridad**
* **14.1.2 Aseguramiento de los servicios de aplicación en las redes públicas**
* **14.1.3 Transacciones en línea**

**Objetivo 2:** Seguridad den los procesos de desarrollo y soporte

Garantizar que la seguridad de la información ha sido diseñada e implementada dentro del ciclo de vida del desarrollo de los de los sistemas de la información.

* **14.2.1 Política de desarrollo seguro**
* **14.2.2 Procedimiento de control de cambio del sistema**
* **14.2.3 Revisión técnica de aplicaciones después de cambios de las plataformas operativas**
* **14.2.4 Restricciones a los cambios en los paquetes de software**
* **14.2.5 Principios de la ingeniería de Sistemas Seguros**
* **14.2.6 Ambiente de desarrollo seguro**
* **14.2.7 Desarrollo subcontratado**
* **14.2.8 Pruebas de seguridad del sistema**
* **14.2.9 Pruebas de aceptación del sistema**

**Objetivo 3:** Datos de prueba

Garantizar la protección de los datos utilizados para las pruebas

* **14.3.1 Protección de datos de prueba**

**OBJETIVO 1: REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**

Se trata de un requisito para la definición y documentación de los requisitos de seguridad para los sistemas de información.

Los controles son los siguientes

**14.1.1 ANÁLISIS Y ESPECIFICACIÓN DE LOS REQUISITOS DE SEGURIDAD**

Deberemos incluir requisitos para la seguridad de la información en la fase de especificación de condiciones para sistemas de información. Esto supone tener en cuenta la seguridad además de las funcionalidades requeridas por una aplicación o sistema antes de su fase de desarrollo.

Los requisitos de seguridad deben tener en cuenta valoraciones del impacto en el negocio de posibles fallos de seguridad (daño potencial)

Tenga en cuenta la principal ventaja de prever requisitos de seguridad en las fases tempranas de un desarrollo es el ahorro de costes ya que un rediseño puede ser mucho más costoso sin contar con los daños potenciales de los fallos no previstos en la seguridad

**¿Qué controles de seguridad debemos considerar en una especificación?**

Para ello podemos tener en cuenta factores como:

* ¿Qué nivel de confianza requiere la aplicación? Con ello podremos determinar los requisitos de autenticación.
* Especificaciones de la provisión de accesos para
  + Usuarios
* Usuarios privilegiados y técnicos de mantenimiento
* ¿Qué funciones y responsabilidades requiere de los usuarios?
* ¿Qué necesidades de protección tienen los activos involucrados? (análisis de riesgos)
* ¿Qué requisitos de seguridad se derivan de los procesos del negocio?
  + Registros de transacciones
  + Supervisión y monitoreo
  + Requisitos de no-repudio
  + Otros
* ¿Qué otros controles de seguridad son aplicables?
  + Interfaces para el registro y supervisión
  + Sistemas de detección de fugas de datos
  + Otros

En el caso de servicios a través de redes públicas hay controles específicos en los puntos siguientes 14.1.2 y 14.1.3

En el caso de compras de aplicaciones a terceros deberíamos establecer como control de seguridad:

* Procesos de compras formales que incluyan periodos de prueba y validación del producto
* Aplicar criterios de evaluación de riesgos para tomar medidas de control adicionales si el producto no satisface totalmente las necesidades de seguridad
* A la hora de integrar un software en aplicaciones o sistemas propios considere si es necesario configurar las aplicaciones, sistemas y Software a implantar en relación a la seguridad. Elabore procedimientos y asegúrese de que se implementan
* Defina protocolos de homologación y aceptación de productos de forma que se incluyan siempre criterios de seguridad de la información
* Aplique los criterios de aceptación de productos en actualizaciones de Software y en nuevas funcionalidades de productos en cuanto a criterios de seguridad. Una nueva funcionalidad puede ser muy interesante pero no debe vulnerar la seguridad de nuestros sistemas para que sea aceptable.

**14.1.2 ASEGURAMIENTO DE LOS SERVICIOS DE APLICACIÓN EN LAS REDES PÚBLICAS**

Si utilizamos redes públicas para la transmisión de información sensible o para acceder a las aplicaciones deberemos tener en cuenta controles adicionales pues las redes públicas como internet suponen un riesgo adicional importante que debemos tener en cuenta si queremos salvaguardar nuestra información

En este caso hemos de valorar:

* El cifrado de las comunicaciones.
* Sistemas múltiples de autenticación.
* Uso de certificados digitales (Identificación segura de origen y destino).
* Sistemas de prevención de envío de información no permitida en redes publicas.
* Sistemas de protección para envíos involuntarios de archivos.

**14.1.3 TRANSACCIONES EN LÍNEA**

Se trata de controles que garanticen la protección de las transacciones entre aplicaciones.

Los controles se han de aplicar para evitar

* Transacciones incompletas
* Errores de enrutamiento
* Mensajes no autorizados
* Alteración de los datos
* Divulgación de la información
* Duplicación de mensajes o reproducción no autorizada.

Para ello deberemos analizar la aplicabilidad de contar con controles tales como

* Uso de firma digital para garantizar las comunicaciones extremo a extremo
* Validación y verificación de autenticación en toda la cadena de transmisión
* El canal de comunicación es cifrado para garantizar la confidencialidad de las transmisiones
* La utilización de protocolos seguros
* Los datos de las transacciones se guardan en lugares no accesibles desde la red (Intranet, Entornos CLOUD etc.)
* La obtención de firmas digitales se debe garantizar que la seguridad se integra e incorpora a través de todo el proceso completo de gestión del certificado o firma.
* De poco valdría trabajar con una autoridad confiable si para obtener los certificados lo vamos publicando al no contar con métodos seguros para obtenerlos

**OBJETIVO 2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE**

Se trata de controles para garantizar que se tienen en cuenta las necesidades de la seguridad de la información en los entornos de desarrollo de sistemas de información

**14.2.1 POLÍTICA DE DESARROLLO SEGURO**

Se deben establecer reglas para que la seguridad de la información sea tenida en cuenta en todo el proceso de desarrollo del software y en todo el ciclo de vida del mismo.

Estas reglas deben tener en cuenta aspectos como

* La seguridad en entornos de desarrollo
* La política determina la metodología que se aplica en el desarrollo del software
* Como se gestionan las distintas versiones de software
* Como se gestionan las vulnerabilidades del software
* Como se asegura los controles de seguridad en software subcontratado
* Como se establecen requisitos de seguridad en la fase de definición de funcionalidades del software

**14.2.2 PROCEDIMIENTO DE CONTROL DE CAMBIO DEL SISTEMA**

Las actualizaciones de software suelen ser el punto crítico a tener muy en cuenta ya que pueden suponer un gran impacto en los entornos de desarrollo. Al igual que los entornos de producción en la fase de desarrollo deberemos vigilar y controlar estrechamente desde la actualización de los navegadores a las actualizaciones de los sistemas operativos y la introducción de nuevas funcionalidades

Para controlar estos cambios deberíamos proceder siempre bajo protocolos establecidos que tengan en cuenta

* El establecimiento de un proceso formal documentado para llevar a cabo los cambios
* La documentación de una especificación técnica o guía sobre la actuación para realizar los cambios
* La realización de pruebas y control de calidad sobre los cambios introducidos
* Gestionar la implementación mediante procesos de autorización, control de permisos y de planificación de los cambios
* La realización de una evaluación de riesgos antes de realizar y planificar los cambios
* Controlar que los requisitos de seguridad de los sistemas afectados no se vean comprometidos en la fase de implementación de los cambios
  + Procesos de aprobación formal
  + Restricción de accesos
  + Control de personal y de tiempos
* Control de versiones de software
* Control de impacto en aplicaciones en servicio
* Limitación de actualizaciones automáticas en aplicaciones criticas

**14.2.3 REVISIÓN TÉCNICA DE APLICACIONES DESPUÉS DE CAMBIOS DE LAS PLATAFORMAS OPERATIVAS**

***“Un paso en falso y al traste con el negocio”***

Después de una actualización deberíamos revisar y probar las aplicaciones para garantizar que los cambios no afecten a su operatividad

Para ello deberíamos tener en cuenta

* Proceso para revisar que se han realizado los cambios según las especificaciones y guías al efecto
* Planificar los cambios para que haya tiempo para realizar las pruebas

**14.2.4 RESTRICCIONES A LOS CAMBIOS EN LOS PAQUETES DE SOFTWARE**

***“¿Actualizar por actualizar?”***

Limitar los cambios en los paquetes software es una buena medida para delimitar o minimizar la posibilidad de generar incidentes. Se trata de limitar las actuaciones sobre el software a cambios absolutamente necesarios

Para ello deberíamos mantener una serie de criterios de actualización de forma que se revisen antes de realizar los cambios o pensar en hacerlos:

* ¿Cuál el riesgo de comprometer los procesos de control y de integridad existentes? Merece la pena correr el riesgo frente a los beneficios que obtendremos con la actualización
* ¿Contamos con el consentimiento o licencia del propietario del software?
* ¿Podemos evitar la actualización con versiones estables y estándar del Software?
* ¿Cuál es el impacto en los recursos sobre el mantenimiento del software a futuro?
* ¿Podemos garantizar la compatibilidad del software a instalar con el software existente?

**14.2.5 PRINCIPIOS DE LA INGENIERÍA DE SISTEMAS SEGUROS**

Los principios de ingeniería seguros nos requieren documentar procedimientos sobre cómo implementar medidas de seguridad en las técnicas de desarrollo como por ejemplo

* Procedimientos seguros para el diseño y codificación (elaboración de código seguro)
* Procesos de diseño de mecanismos de autenticación difíciles vulnerar
* Procesos de somatización de variables
* Procedimientos para el uso correcto de la criptografía
* Etc.

**14.2.6 AMBIENTE DE DESARROLLO SEGURO**

La evaluación de riesgos para la seguridad de la información no solo debe afectar a los activos de información como software, datos o equipos y soportes sino que también debe aplicarse a los entornos de desarrollo, las personas, los procesos de desarrollo y las tecnologías utiliza dadas para determinar si es necesario aplicar medidas o controles de seguridad

Para evaluar si son necesarias controles de seguridad a las personas o procesos deberíamos tener en cuenta

* El grado de sensibilidad de los datos
* Los niveles de seguridad aplicables
* Los controles de seguridad definidos para cada tipo de información
* La confiabilidad del personal (ver 7.1.1)
* Las necesidades de separar entornos de desarrollo
* Los controles de acceso determinados para el entorno de desarrollo
* Las necesidades de respaldo de información
* Los controles y políticas para el traslado de información

**14.2.7 DESARROLLO SUBCONTRATADO**

Para la subcontratación de desarrollos de Software deberíamos tener en cuenta

* Establecer y supervisar el cumplimiento de los requisitos de seguridad
* Controlar y gestionar todos los aspectos de licencias y propiedades de código fuente
* Metodología y definición de las pruebas a realizar al software subcontratado
* Todo lo anterior debe ser plasmado en acuerdos firmados y consensuados con el proveedor

**14.2.8 PRUEBAS DE SEGURIDAD DEL SISTEMA**

Los requisitos para la seguridad de un sistema software deben ser probados como si se tratase de una funcionalidad más del software. Para ello debería implementarse un plan de pruebas documentado.

Las pruebas también deben incluir al software subcontratado

**14.2.9 PRUEBAS DE ACEPTACIÓN DEL SISTEMA**

El proceso de incorporación de nuevas aplicaciones actualizaciones o nuevas versiones de software debe estar sujeto a un proceso de aceptación donde se le realicen las pruebas funcionales y de seguridad planificadas.

Los entornos de pruebas deben ser distintos a los entornos de operación para evitar fallos en sistemas reales

**OBJETIVO 3 DATOS DE PRUEBA**

Los entornos de pruebas no siempre cuentan con los mismos niveles de seguridad que los entornos de operación por lo que se deberían establecer controles para seleccionar los datos para los sistemas de prueba o entornos de desarrollo

**14.3.1 PROTECCIÓN DE DATOS DE PRUEBA**

Si no existe otra posibilidad en los entornos de prueba deberíamos utilizar datos NO reales para los desarrollos y pruebas posteriores de los sistemas.

En caso de que esto no fuera posible deberíamos aplicar los mismos controles de seguridad (acuerdos de confidencialidad etc.) que aplicamos a los datos reales

**A15 RELACION CON PROVEEDORES**

En caso de que empresas o personal externo a la organización tengan acceso a los sistemas de información o a los recursos que manejan activos de información deberemos establecer de modo formal las condiciones para el uso de dichos activos y supervisar el cumplimiento de dichas condiciones

Veamos los objetivos y los controles establecidos para ello en ISO 27001.

Citando la norma:

**Objetivo 1:**  
Seguridad de la información en las relaciones con los proveedores

Garantizar la protección de los activos de la organización, que sean accesibles por los proveedores.

* **15.1.1 Política de seguridad de la información para las relaciones con los proveedores**
* **15.1.2 Tener en cuenta la seguridad en los acuerdos con proveedores**
* **15.1.3 Cadena de suministro de tecnologías de la información y las comunicaciones**

**Objetivo 2:**  
Gestión de la entrega del servicio por terceras partes

Mantener un nivel apropiado de seguridad de la información y la entrega del servicio acorde con los acuerdos por sus terceras partes.

* **15.2.1 Seguimiento y revisión de los servicios de proveedores**
* **15.2.2 Gestión de cambios en los servicios de los proveedores**

**OBJETIVO 1: SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES**

Cuando el acceso a la información se realiza por parte de personal externo se plantean nuevos escenarios de riesgo para la seguridad de la información.

Este capítulo también tiene que ver con los servicios que contratamos para almacenar nuestros datos y aplicaciones. Cada vez es más común que las empresas contraten de forma externa el alojamiento de servidores, aplicaciones datos y servicios de comunicación. Esto genera un panorama completamente nuevo en cuanto a los riesgos generados para la seguridad de la información.

Para mitigar estos importantes riesgos se nos propone analizar la aplicabilidad de los siguientes controles

**15.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES**

La relación con un proveedor normalmente está regulada por un contrato de prestación de servicios. Entonces es aquí donde deberíamos reflejar las condiciones para el manejo adecuado de la información de nuestra organización de acuerdo con los requisitos de seguridad que hayamos definido.

Las condiciones de seguridad deben ser acordadas con el proveedor antes de firmar los contratos y debe quedar documentada si es necesario en los anexos oportunos.

No debe pasar por alto…

*… que los proveedores tendrán acceso a la información confidencial de su empresa.*

*Por ejemplo, si su empresa subcontrata el desarrollo de una aplicación Software para prestación de sus servicios es muy posible que el proveedor conozca el plan estratégico de su negocio, los procesos de su empresa y además tenga acceso a los datos en tiempo real de sus clientes y contactos etc., lo mismo ocurre si usa servicios en la nube.*

*Sus proveedores conocerán entonces qué es lo más valioso de su empresa;*

***¡Como para no tomarse en serio este punto!***

Tampoco se olvide de …

*Sus socios o partners en el negocio que por diversos motivos pueden manejar información sensible de su empresa, datos de sus clientes y proyectos, información sobre desarrollos de productos etc.*

*¿Sus CLIENTES TAMBIEN? no es poco frecuente que potenciales clientes nos pidan datos sobre nuestra empresa antes de firmar ningún contrato, sin ir más lejos en las licitaciones se suele pedir mucha información sobre productos, estructura empresarial, precios, incluso información sobre procesos o auditorias previas a una posible relación comercial*

***¡Todo esto hay que tenerlo en cuenta para poner siempre cláusulas de confidencialidad y los controles de seguridad que podamos aplicar!***

En este punto entonces es fundamental no saltarse los pasos del proceso para proteger nuestra información



*Analizar los riesgos*

Ante la subcontratación de procesos que implican el acceso a la información deberemos evaluar los posibles impactos que puede tener en la seguridad de la información

Subcontratar servicios de información tiene muchos beneficios hoy en día para la empresa como la reducción de costes la mayor flexibilidad etc. sin embargo tengamos en cuenta que riesgos plantea:

Si nuestro proveedor como hemos visto puede acceder a información estratégica de nuestra empresa, esto puede originar una situación comprometida para la seguridad de la información con un riesgo potencial de que se produzcan fugas de información cuyo origen sea nuestro proveedor. En este caso mantener a raya estos riesgos dependerá de las medidas de seguridad que haya implantado nuestro proveedor y del control que ejerzamos sobre ello.

Para evaluar los riesgos hemos de analizar que activos de información están afectados por la subcontratación o cesión de datos a terceros y analizar las posibles amenazas y el impacto que tendrían su pérdida de confidencialidad, integridad o disponibilidad.

Se trata pues de seguir el proceso de evaluación de riesgos para cada activo: aplicación, servicio, tareas o procesos que hayamos subcontratado o tengamos intención de hacerlo

Para más detalles sobre cómo realizar el análisis de riesgos

No debe pasar por alto…

*"Los resultados de la revisión de la gestión deben incluir decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambios en el sistema de gestión de seguridad de la información"*

*… Dentro de los riesgos no está solamente la degradación de la información sino a veces el propio control de la información.*

*Por ejemplo, si subcontratamos un servicio de ciberseguridad a un proveedor externo, el control sobre los incidentes en la seguridad de la información pasaría a estar de forma indirecta por lo que pueden pasarse por alto incidentes simplemente por estar mal informados, por lo que tendremos una percepción totalmente distorsionada del riesgo al que estamos sometidos.*

*Al subcontratar servicios también podemos tener una pérdida de conocimiento sobre nuestro propio negocio “Know-how” ya que mucha información relativa no solo a la resolución de incidencias, sino también a las oportunidades de mejora, rendimiento de los sistemas etc. puede quedar oculto a nuestros ojos si no le ponemos remedio.*

***Todo esto debe formar parte también del análisis de riesgos para poder luego tomar acciones para evitarlo***



*Selección de Conrtroles*

El segundo paso como ya conocemos es el análisis o auditoria de los controles que deberíamos aplicar a los activos identificados para evitar o mitigar los riesgos identificados.

Estos controles pueden ir desde la investigación de los antecedentes de nuestros socios y proveedores, verificando información financiera, antecedentes penales, auditorías de controles y procesos de seguridad del proveedor etc.

Defina pues un proceso claro sobre la contratación que tenga en cuenta estas evaluaciones.

Tenga en cuenta los controles de seguridad que podemos establecer en los acuerdos de prestación de servicios 15.1.2

Tenga en cuenta siempre que las investigaciones realizadas deben mantenerse dentro de la legalidad vigente y cumplir con las leyes de protección de datos.



*Acuerdos de Prestación de Servicios*

Una vez identificados los controles de seguridad a aplicar tenemos que plasmar estos controles en los acuerdos de confidencialidad, algo que trataremos en detalle en el próximo punto mediante un caso práctico que nos ayudara a desarrollar este punto.



*Control de Accesos*

No se olvide de definir una política de control y restricción de los accesos a la información. Esto puede ser una herramienta que nos ayude a mantener el riesgo más controlado evitando en todo momento el acceso a innecesario a la información.

El criterio es el de siempre de la mínima información necesaria para el desarrollo de los trabajos. Esto podemos aplicarlo tanto al ámbito físico como lógico.



*Monitoreo*

Podemos poner muchos y estupendos controles pero si nos olvidamos de supervisar si se están cumpliendo podemos quedarnos a medias en nuestra tarea.

Es por eso que debe supervisar y, si es necesario, auditar si cumplen con todas las cláusulas; por ejemplo, si acordaron con el proveedor dar el acceso a sus datos solo a un número determinado de sus empleados, esto es algo que debe verificar.



*Finalización del Servicio*

No olvidemos que las finalización de los acuerdos de servicio, trabajos o relación contractual no supone la finalización de las obligaciones en materia de confidencialidad, algo que debe estar contemplado en las clausulas o anexos del contrato de prestación de servicios.

Por otro lado, deberemos establecer controles para la:

* La devolución de los activos de información
* La eliminación o destrucción de datos
* La cancelación y revocación de los accesos

**15.1.2 TENER EN CUENTA LA SEGURIDAD EN LOS ACUERDOS CON PROVEEDORES**

Las condiciones de seguridad de la información deben quedar reflejadas en los contratos de forma explícita y en un apartado específico para ello.

Los documentos sobre los acuerdos para la seguridad de la información deben estar firmados por ambas partes.

A continuación les dejamos un ejemplo o listado de requisitos de seguridad que pueden exigir a un proveedor:

CASO PRACTICO  
REQUISITOS DE SEGURIDAD A PROVEEDORES

REQUISITOS GENERALES

***RESPONSABLE DE SEGURIDAD***

*Requiera a su proveedor la designación de un responsable de seguridad quien servirá de interlocutor para cualquier tema de seguridad y el responsable de que se cumplan los controles pactados entre las partes*

***CONTROL DE PERSONAL***

*Requiera a su proveedor que le mantenga informado de cualquier cambio de personal dedicado a la prestación de servicios dentro del acuerdo firmado. Defina como y cuando se realizaran las comunicaciones.*

*Establezca un requisito para que el personal que ha sido dado de baja se le han revocado los permisos de acceso tanto a las instalaciones como a los sistemas de información.*

***REQUISITOS LEGALES***

*Asegúrese de que el proveedor cumple los requisitos legales sobre el negocio, protección de datos etc. Obtenga su compromiso por escrito*

***USO DE ACTIVOS***

*Ponga por escrito una clausula que hable del uso correcto de sus activos donde el proveedor se compromete al uso de los activos para la finalidad prevista y que tomara las medidas de control que se establezcan para evitar el daño o revelación de la información y los accesos no autorizados.*

***AUDITORIAS DE SEGURIDAD***

*Establezca condiciones para la disponibilidad del contratista para la realización de auditorías de seguridad tanto en instalaciones como al personal y procedimientos o controles de seguridad.*

***CONTROL DE PROCEDIMIENTOS***

*Establezca clausulas específicas para que el proveedor mantenga procesos de seguridad*

*Aquí les dejamos un ejemplo:*

* *Procesos de contratación*
* *Procesos de devolución o destrucción de la información a la finalización del acuerdo.*
* *Planes de formación en seguridad de la información*
* *Procesos de control de cambios*
* *Procesos de tratamiento de incidencias u no conformidades*
* *Procesos de escalado en la resolución de incidencias*
* *Procesos de actualización de software y programas de seguridad (antivirus firewall etc.)*
* *Planes de emergencia y de recuperación de desastres*
* *Otros*

CONTROL DE SOFTWARE MALICIOSO (VIRUS)

*Establezca requisitos para el control de virus y software malicioso de equipos y soportes que se conecten a la red de su empresa y a la obligación de mantener un control de antivirus actualizados.*

*Asegúrese de que el proveedor ha tomado medidas de control (escaneo de virus) y establecido políticas para los usuarios sobre el uso de redes, emails, aplicaciones etc. que prevengan el software malicioso.*

USO DEL SOFTWARE

*Pacte cláusulas que exijan en cualquier equipo que se conecte a la red de su organización.*

* *USO de Software autorizado*
* *Prohíba el uso de software privado*
* *Instalación y uso de software gratuito*
* *Uso de software sin licencia*

GESTION DE INCIDENTES

*Establezca clausulas para*

* ***Una descripción de la ubicación de los activos que incluya planos de planta para describir el perímetro***
* ***Descripción de las unidades organizativas, por ejemplo mediante organigramas***

GESTION DE CAMBIOS

*Documente la obligación de ceñirse al control de cambios de su organización para que cualquier cambio gestionado por el contratista quede reflejado en el registro de cambios establecido y se realice de acuerdo a sus procedimientos*

DESARROLLO DE SOFTWARE

*Establezca clausulas para controlar el desarrollo de software de su proveedor.*

*Aquí dejamos algunos ejemplos:*

* *Prohibición de uso de accesos maestros (puertas traseras)*
* *Obligaciones de documentación de funcionalidades, uso, configuración*
* *Cumplimiento de las normas de seguridad corporativas de su empresa*
* *Previsión de módulos o accesos especiales para realización de auditorias*
* *Cumplimiento de las políticas corporativas de requerimientos de seguridad definidas para el software*
* *Otros*

EQUIPOS INFORMATICOS

*Por ejemplo, se pueden establecer clausulas para que los portátiles que prestan servicio estén protegidos contra robo con sistemas de cifrado y acceso por huella digital*

AUTENTICACION

*Establezca requisitos para*

* *Determine requisitos para el uso de contraseñas*
  + *Tiempo máximo de validez de contraseñas*
  + *Prohibición de reutilizar contraseñas*
  + *Prohibición de compartir contraseñas*
  + *Necesidad de cambiar contraseñas cuando se hayan compartido por necesidades de trabajo*
* *Determine las funciones del responsable de seguridad a la hora de gestionar contraseñas otorgadas para el uso por parte del contratista*
* *Establezca cual es el criterio mínimo en la seguridad de contraseñas*
  + *Por ejemplo: mínimo 8 caracteres al menos 1 en mayúscula y que contenga números y letras*
  + *Prohíba que las contraseñas tengan nombres propios, partes de números de teléfono, fechas de nacimiento etc.*
* *Establezca los criterios con los que deben ser gestionadas las contraseñas cuando pasan por el responsable de seguridad y van destinadas a otras personas*
  + *Forzar cambios de contraseñas*
  + *Métodos seguros de entrega y custodia*
  + *Identificación del usuario final mediante ID*
  + *Responsabilidades por el incumplimiento (Por ejemplo. El contratista será responsable de los daños causados por el incumplimiento de las normas de gestión de contraseñas contenidas en este apartado y de las responsabilidades legales establecidas por la compañía)*

USO Y CONEXIÓN DE REDES INFORMATICAS

*Establezca pautas para la conexión y transmisión de datos cuando sea aplicable a su contratista. Por ejemplo:*

*Establezca la necesidad de utilizar protocolos seguros de transmisión cuando el contratista deba transmitir datos con información reservada o información interna de la compañía (Por ejemplo utilizando redes VPNs basadas en IPSEC o SSL)*

*Requiera el uso de SSL en los controles de acceso remoto*

*Evite que su contratista use protocolos no seguros como FTP, Telnet, rlogin, rexec, rsh, vnc*

*Requiera que el contratista tenga a las mismas personas en la operación y en la asignación o gestión de controles de acceso (contraseñas etc.)*

*Exija el uso de firewalls en cualquier conexión con redes externas y restringa el uso de módems y dispositivos similares como ADSL etc. en redes o sistemas que estén conectados a las redes internas de su compañía*

*Establezca criterios técnicos para la configuración y funcionalidades de los firewalls*

*Establezca clausulas para definir expresamente los comportamientos anómalos en los intentos de conexión a las redes de la compañía (por ejemplo prohibición de uso de comandos “ping” o cualquier sistema de intento de conexión no autorizada*

*Establezca claramente la necesidad de que cualquier dispositivo a conectar a la red interna de la compañía debe estar sujeto a autorización*

*Requiera que todos los dispositivos que se conectan a la red interna este continuamente atendidos*

*Controle mediante una clausula que no se permitirá la realización de cambios en ningún sistema o equipo de la compañía, en cuanto a cambios de software, código etc. salvo los que estén expresamente autorizados y programados*

*Los permisos de accesos a los sistemas de información deben ser tramitados siempre ante el propietario de os activos de información los cuales serán informados por la compañía al contratista así como los procedimientos para las autorizaciones*

*Especifique la necesidad de devolver los dispositivos de acceso e identificaciones al terminar las actividades.*

OBLIGACIONES DEL PERSONAL

*Especifique las obligaciones a las que están sujetas las personas que presten servicio dentro del acuerdo. Por ejemplo:*

*Cumplir con las obligaciones de seguridad de la compañía especificando el documento donde se encuentran.*

*Establezca como obligación conocer y seguir las recomendaciones de los planes de emergencias y de respuesta ante los incidentes de seguridad de la información de la compañía (especifique documento).*

*Establezca obligaciones en el cumplimiento de la gestión de identificaciones y credenciales de acceso, uso de contraseñas etc.*

* *Obligaciones de custodia*
* *Obligaciones de uso de contraseñas seguras*
* *Obligaciones de renovación de contraseñas*
* *etc.*

*Obligaciones de cumplir con las políticas de escritorio*

* *Cerrar las sesiones*
* *Escritorios limpios*
* *Destruir información impresa*
* *Guardar bajo llave información sensible*
* *Protección de portátiles*
* *Atención a las impresoras y faxes*
* *Etc.*

*Obligaciones sobre la propiedad intelectual*

* *Cumplir con las restricciones de propiedad intelectual del software*

*Obligaciones sobre la ley de protección de datos personales*

*Cumplir con las recomendaciones para los accesos de teletrabajo*

*Obligaciones sobre el uso de activos de información, custodia, finalidad, devolución etc.*

*Obligaciones de confidencialidad y no divulgación*

*En este apartado ponga clausulas para que el personal tenga el compromiso por escrito de mantener la confidencialidad de*

* *Documentos*
* *Métodos de trabajo*
* *Claves y contraseñas*
* *Programas y Software*
* *Información en general*
* *Etc.*

*Determine por escrito la obligación de no divulgar la información y de mantener el acuerdo aun después de terminar la relación contractual*

OBLIGACIONES SOBRE LAS INSTALACIONES

*Establezca requisitos para la seguridad en el trabajo en sus instalaciones tales como*

* *Uso de identificaciones en todo momento*
* *Cumplir con los controles de acceso*
* *Defina comportamientos no permitidos dependiendo en que instalaciones (comida, bebidas, fumar etc.)*
* *Cumplir con las políticas de buen uso de las instalaciones*
* *ETC*

**15.1.3 CADENA DE SUMINISTRO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES**

La norma en este punto nos pide que tengamos en cuenta requisitos de seguridad de la información no solamente a nuestros proveedores sino que fijemos los requisitos para toda la cadena de suministro. Es decir, los riesgos para la seguridad de la información también están afectados por lo que nuestros proveedores subcontraten.

Los dos principios para sostener una cadena de suministro con garantías son

* Proveedores de confianza.
* Exigir a los proveedores un control de seguridad a sus propios proveedores.

Los controles que podemos observar aplicados a la cadena de suministro son:

* Establecer los criterios de seguridad para cada servicio, producto o tecnología de comunicación a subcontratar. La evaluación de riesgos enfocada a un servicio o producto en concreto, nos puede ayudar a establecer los criterios a la hora de subcontratar este servicio y determinar qué características o nivel de seguridad requiere a la hora de elegir al contratista.
* Establecer clausulas para el subcontratista en cuanto a que apliquen requisitos de seguridad a sus proveedores y a toda la cadena de suministro.
* Este apartado no dejaría de ser una declaración de intenciones si no se detallan que partes de los productos o servicios subcontratados a su vez requieren de otros proveedores externos y que requisitos y controles de seguridad se van a aplicar para garantizar la seguridad de la información
* Finalmente no nos queda otra que establecer procesos para comprobar que los productos o servicios suministrados cumplen con los requisitos establecidos para la seguridad de la información al menos para los productos y servicios que determinemos como fundamentales y que son adquiridos fuera de la organización.
* Exigir la trazabilidad de componentes críticos
* Establecer un proceso para comunicarnos con nuestros proveedores y la cadena de suministro
* Por ultimo no nos olvidemos que hoy en día los desarrollos, componentes y aplicaciones entran en obsolescencia o quedan fuera del suministro por parte de proveedores.

No debe pasar por alto:

*Hoy en día los componentes, aplicaciones, sistemas operativos tienen también un ciclo de vida determinado en cuanto a su mantenimiento en el mercado por lo que la gestión de la obsolescencia de los productos adquiridos a terceros pasa por realizar un análisis de riesgos del ciclo de vida de componentes y aplicaciones de modo que*

* *Preveamos acopio de materiales sensibles que puedan quedarse fuera de fabricación*
* *Preveamos desarrollos o alternativas a dichos productos*
* *Tengamos previstos los impactos de costes de la obsolescencia de productos tanto componentes como aplicaciones.*
* *Tengamos en cuenta el riesgo para la seguridad de la información si mantenemos versiones de sistemas operativos que ya no se actualizan ni mejoran su seguridad.*

**OBJETIVO 2 GESTIÓN DE LA ENTREGA DEL SERVICIO POR TERCERAS PARTES**

Mantener un nivel apropiado de seguridad de la información y la entrega del servicio acorde con los acuerdos por sus terceras partes.

Derivado de la lógica de los sistemas de gestión, todo control no solo debe establecerse, sino que además tendremos que mantenerlo a lo largo del tiempo. El tema del control de los proveedores sigue el mismo patrón. No solo vale poner requisitos, sino que además hay que verificar que se cumplen a lo largo del tiempo por lo que será necesario controlar los servicios prestados y los cambios en los mismos.

**15.2.1 SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE PROVEEDORES**

Siempre que se pueda y el esfuerzo no sea desproporcionado deberemos establecer mecanismos de monitorización de los servicios proporcionados por terceros y además solicitar los informes al proveedor sobre el nivel de servicio prestado.

**15.2.2 GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES**

Cuando modificamos los servicios prestados por proveedores deberíamos controlar

* Aplicar un análisis de riesgos al nuevo escenario
* Evaluar la necesidad de modificar o ampliar los acuerdos de prestación de servicios para cubrir las nuevas necesidades de seguridad si así se estima oportuno

# A16 GESTION DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACION

Los incidentes en la seguridad de la información parecen inevitables hoy en día por lo que no tenemos más remedio que plantearlos como vamos a gestionar dichos incidentes de la manera más ágil y eficiente para la organización

Es por ello que la norma **ISO 27001** dedica un capítulo a establecer controles para gestionar los incidentes en la seguridad de la información e inclusive se ha dedicado un documento específico con los principios para gestionar incidentes en la seguridad de la información

Citando la norma:

**Objetivo 1:**  
Gestión de incidentes y mejoras de seguridad de la información

Garantizar un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades. .

* **16.1.1 Responsabilidades y procedimientos**
* **16.1.2 Reporte de eventos de seguridad de la información**
* **16.1.3 Reporte de debilidades de seguridad de la información**
* **16.1.4 Evaluación y decisión sobre los eventos de seguridad de información**
* **16.1.5 Respuesta a incidentes de seguridad de la información**
* **16.1.6 Aprendiendo de los incidentes de seguridad de la información**
* **16.1.7 Recolección de evidencia**

## OBJETIVO 1: GESTIÓN DE INCIDENTES Y MEJORAS DE SEGURIDAD DE LA INFORMACIÓN

Como hemos mencionado, un análisis de riesgos no puede concluir con la eliminación total de las vulnerabilidades pues esto aún ni siquiera seria práctico o viable por lo que las vulnerabilidades residuales siempre existen por lo que tendremos de seguro incidentes en la seguridad de la información además de que puedan surgir amenazas o y vulnerabilidades no identificadas hasta ahora.

Es por ello que debemos implementar una herramienta para la gestión de los incidentes de la seguridad de la información con los siguientes objetivos generales

* **Detectar**, informar y evaluar incidentes de la Seguridad de la información
* **Responder** a incidentes
* **Reportar** vulnerabilidades
* **Aprender** de los incidentes de la Seguridad de la información

**LOS PASOS PARA LA RESOLUCION DE INCIDENTES**

La gestión de incidentes de seguridad se basa en diferentes pasos, que incluyen:



NOTA: Estos pasos podrían ser estados diferentes que un incidente por lo que también es importante informar al usuario sobre cualquier cambio en el estado del incidente.

* **1. Notificación del incidente:** una persona detecta un evento que puede dañar el funcionamiento de la organización, por lo que necesita comunicar el incidente de acuerdo con los procedimientos de comunicación de la organización (generalmente un correo electrónico, una llamada telefónica, una herramienta de software, etc.)
* **2. Clasificación del incidente:** una persona recibe la notificación del incidente y, según los diversos parámetros, se clasifica. La persona que detecta el incidente también puede hacer una clasificación, pero es un experto técnico que lo clasifica de la manera adecuada.
* **3. Tratamiento del incidente:** una vez que se clasifica el incidente y se conoce la gravedad y el tiempo acordado para su resolución, un experto técnico debe decidir sobre las medidas necesarias para resolverlo.
* **4. Cierre el incidente:** una vez que se resuelve el incidente, se registra toda la información generada durante el tratamiento y, finalmente, se notifica a la persona que envió primero la notificación del incidente que se cerró.
* **5. Base de conocimiento:** toda la información generada durante el tratamiento del incidente es crítica para posibles incidentes similares en el futuro, así como para recopilar evidencia. Imagine que un usuario actualiza un sistema y luego de esto, el sistema se cierra (involuntariamente). Luego, el usuario abre un incidente y el incidente se resuelve y se cierra. La información generada para resolver el incidente se registra, por lo que si el problema vuelve a ocurrir en el futuro, simplemente pueden referirse a la base de conocimiento; Tendrán la solución perfecta sin perder tiempo.

En este sentido la norma establece una serie de controles empezando por la organización que debemos llevar a cabo para acometer esta tarea

**CONTROLES PARA LA GESTION DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACION**

### 16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS

En primer lugar deberemos tener implantado y documentado los procedimientos que nos dirijan en el proceso de gestión de incidentes de la seguridad de la información,

Estos procesos deben tener en cuenta

* **Las responsabilidades**
  + Defina un responsable o responsables para la gestión de incidentes quien deberá garantizar que se desarrollan los procedimientos adecuados para que se realicen todas las tareas o procesos necesarios para gestionar los incidentes
  + Defina las responsabilidades de cada empleado tanto en la colaboración para la respuesta, como en la necesidad de comunicación de los incidentes de seguridad de la información
* **Los procesos o procedimientos**
  + Que existan procedimientos para la detección, análisis y elaboración de informes de incidentes de la seguridad de la información
  + Elabore procedimientos para que se comuniquen los incidente
  + Que dichos procedimientos sean conocidos (Que cada empleado conozca los procedimientos de comunicación de incidentes y sus responsabilidades)
  + Que existan vías de comunicación adecuadas (asegúrese de que se definen los puntos de recogida de información para los incidentes y eventos de la seguridad de la información)
* **Capacitación**
  + Asegúrese de la competencia del personal de atención y resolución de incidentes. Mantenga un plan de capacitación de las personas que se ocupan de los incidentes de la seguridad de la información

### 16.1.2 REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

Este control nos pide que establezcamos los canales de comunicación para todos los eventos o incidentes. Estos canales, naturalmente deben estar establecidos con los responsables de la gestión de los incidentes.

Es importante que todos los usuarios estén informados y familiarizados con los mecanismos de notificación. Con usuarios nos referimos a usuarios tanto internos como externos

Antes que nada vamos a distinguir entre dos conceptos más o menos similares pero que debemos separar para un correcto análisis de los incidentes en la Seguridad de la Información

**EVENTO EN LA SEGURIDAD DE LA INFORMACION**

Cualquier ocurrencia identificada en un sistema de información, servicio o estado de la red que indica una posible infracción en la seguridad de la información, en la política o fallo en los controles, o una situación previamente desconocida que puede ser relevante para la seguridad

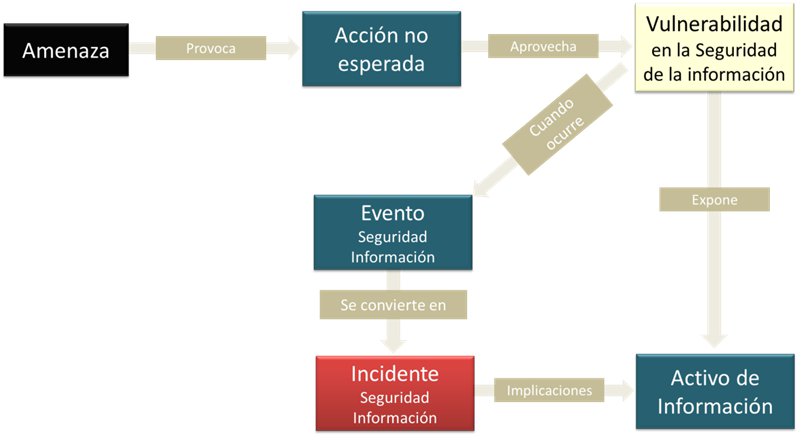
**INCIDENTE EN LA SEGURIDAD DE LA INFORMACION**

Cuando el evento se puede clasificar como no deseado o inesperado dentro de los eventos de seguridad de la información y además tienen una probabilidad significativa de comprometer las operaciones comerciales y suponen una seria amenaza para la seguridad de la información

Un evento en la seguridad de la información no significa necesariamente una implicación en la confidencialidad, integridad o disponibilidad a veces incluso lo deseamos, podemos aprender de ello y endurecer la seguridad

El incidente siempre es indeseado

#### **ACLARANDO CONCEPTOS: AMENAZA, VULNERABILIDAD, EVENTO E INCIDENTE**



Definición:  
Amenaza para la Seguridad de la información

*Una amenaza se refiere a cualquier cosa que tenga el potencial de causar daños graves a un sistema o activo de información. Una amenaza es algo que puede suceder o no, pero tiene el potencial de causar un daño grave.*

*Las amenazas pueden provocar ataques a sistemas informáticos, redes y más.*

Definición:  
Vulnerabilidad en la Seguridad de la información

*Se refiere a una debilidad o defecto en un sistema o activo de información que puede dejarlo expuesto a una amenaza o ataque. Una vulnerabilidad también puede referirse a cualquier tipo de debilidad en un sistema de información en sí mismo, en un conjunto de procedimientos o en cualquier cosa que deje la seguridad de la información expuesta a una amenaza.*

Definición:  
Evento en la Seguridad de la información

*Un evento de seguridad de la información es un cambio en las operaciones diarias de una red o servicio de tecnología de la información que indica que una política de seguridad puede haber sido violada o una protección de seguridad puede haber fallado.*

Definición:  
Incidente en la Seguridad de la información

*Una sola o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar seguridad de información. Por ejemplo un comportamiento anómalo en un sistema es un evento, sin embargo, si se encuentra evidencia del virus en el sistema, se puede considerar un incidente de seguridad.*

### 16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN

El reporte de incidentes debe acompañarse con un reporte de posibles debilidades del sistema que se detecten en cualquier momento. Esto debe estar soportado por:

* La comunicación a los usuarios de la exigencia de observar y reportar cualquier debilidad de seguridad de la información vista o sospechada en sistemas o servicios

Se aconseja advertir que los usuarios que probar la fortaleza o debilidad de los sistemas a ver si encuentran una vulnerabilidad serán considerados por la compañía como un mal uso del sistema

### 16.1.4 EVALUACIÓN Y DECISIÓN SOBRE LOS EVENTOS DE SEGURIDAD DE INFORMACIÓN

Como ya hemos visto en los puntos anteriores, los eventos de la seguridad de la información pueden clasificarse en simples eventos o pueden pasar a ser Indecentes de la seguridad de la información

Para ello establezca:

* Un criterio de priorización de incidentes dependiendo del sistema o servicio afectado, del usuario etc.
* La evaluación de incidentes debe ser realizada tanto por el usuario como por el equipo de gestión que debe revisar la prioridad.
* Lleve un registro de la evaluación de los incidentes para poder analizar los parámetros de calidad tanto en su resolución como de su clasificación.

Hay muchas formas de clasificar incidentes, pero lo habitual es considerar dos parámetros:

* **Impacto:**  
  Daño causado al negocio (en términos económicos, imagen, etc.)
* **Urgencia:**  
  La rapidez con la cual la organización necesita corregir el incidente

La combinación de estos parámetros nos permitirá determinar la prioridad de cada incidente, por lo que de esta manera puede establecer, por ejemplo, la siguiente tabla de valores:



Así podríamos clasificar las incidencias en:

* **NIVEL CRÍTICO (5 a 6)**\_\_
* **NIVEL GRAVE (4)**\_\_
* **NIVEL LEVE (1 a 2)**\_\_

### 16.1.5 RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Se trata de controlar el proceso de resolución de incidentes en la seguridad de la información.

Los controles a establecer serian.

* Evalúe si la organización tiene la capacidad para resolver el incidente por si misma o necesita ayuda de terceros.
* Mantenga un registro con las evidencias de las incidencias
* Establezca el sistema de comunicaciones necesarias entre usuarios y el equipo de gestión de incidencias o quien deba estar informado de las actuaciones y situación del proceso de resolución de las incidencias
* Registre las acciones llevadas a cabo y los resultados de las mismas
* Cierre la incidencia formalmente cuando se haya resuelto
* Realice un análisis para determinar las causas de cada incidente

### 16.1.6 APRENDIENDO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Como ya hemos adelantado los incidentes no solo son un problema a solucionar sino una fuente de información para la resolución de futuros incidentes o para la mejora de la seguridad de la información

Los controles de la norma para mantener una base de conocimientos sobre los incidentes en la seguridad de la información son:

* Creación de un registro que considere
  + Volumen de incidentes producidos
  + Tipología de incidentes producidos
  + Coste de la resolución de la incidencia
  + Impacto de la incidencia
  + Solución aplicada

La información sobre los incidentes nos puede ayudar a

* Identificar los incidentes más recurrentes y de alto impacto
* Mejorar nuestro sistema de gestión con nuevos controles y criterios para la evaluación de riesgos
* Realizar entrenamientos a los usuarios para evitar incidentes y a los gestores de incidentes para mejorar la resolución de los mismos

Para este último punto se recomienda utilizar datos No reales para los entrenamientos.

### 16.1.7 RECOLECCIÓN DE EVIDENCIA

Los incidentes sobre la seguridad de la información pueden requerir acciones posteriores como sanciones o acciones legales. Recuperar las evidencias para utilizarlas posteriormente puede volverse un dolor de cabeza si no hemos previsto algún mecanismo para guardarlas.

En este capítulo la norma nos pone como control el que conservemos la información sobre las incidencias de forma que podamos recuperar:

* Los inicios y cierres de sesión
* Las identificaciones
* El estado de los dispositivos y de las redes
* Las evidencias de reuniones informativas, documentación sobre responsabilidades y funciones de seguridad del personal

No debe pasar por alto…

*En ocasiones puede ser necesaria una investigación forense de las evidencias informáticas. Conviene tener en cuenta mantener a salvo los derechos de acceso a la información para poder realizar una investigación forense.*

*Para ello hay que tener en cuenta los distintos requisitos de las jurisdicciones pertinentes y estar preparados mediante la comunicación previa al personal o la firma de cláusulas contractuales*

Otro tema es la preservación de las evidencias…

*Los incidentes no sabemos normalmente en que van a terminar y si requerirán posteriores acciones legales o disciplinarias Determinadas incidencias pueden conllevar el borrado de las evidencias con el objeto de ocultar al responsable de las mismas, es por ello que se recomienda establecer sistemas de copiado y preservación de registros con tal de que ciertas evidencias no se puedan eliminar tan fácilmente.*

Seguridad de las evidencias…

*Finalmente si es posible o se identifica como necesario se pueden certificar los sistemas de recogida de evidencias o mantener medios de vigilancia y control independientes (homologados y legales) para fortalecer las evidencias de cara a acciones legales*

**A17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO**

La continuidad del negocio dentro de los requisitos de la norma ISO 27001 debe ser tratada como una herramienta para dar respuesta a las amenazar que una organización puede sufrir en cuanto a inundaciones, actos vandálicos, incendios y otras amenazas similares

Se trata de implantar medidas de protección y de recuperación ante posibles desastres de esta naturaleza para minimizar los daños y facilitar el restablecimiento de las operaciones.

Mantener un plan de continuidad o recuperación ante incidentes puede ser la clave de la supervivencia en muchas organizaciones

ISO 27001:2013 incorpora en su nueva versión un capitulo que nos aclara como implantar el plan de continuidad del negocio en una organización enfocándose en los aspectos de la seguridad de la información.

**ISO 27001 e ISO 22301**

En anteriores versiones quedaba poco claro como implantar un sistema de continuidad del negocio dentro de la norma ISO 27001 máxime cuando ISO saco la norma específica sobre este aspecto: ISO 22301 Gestión de la continuidad del Negocio

Aquí queremos despejar algunas dudas que pueden surgir al respecto de este punto

* ¿Necesitamos un Sistema de Gestión de Continuidad de Negocio que cumpla con ISO 22301 para obtener la certificación ISO 27001?
* ¿El certificado ISO 27001 nos garantiza que la organización cuenta con un sistema razonable de gestión de la continuidad del negocio?

Veamos cómo responder a esas cuestiones previas

* 1. Los únicos elementos sobre la gestión de la continuidad de negocio que deben tenerse en cuenta en ISO 27001 son los específicos de la continuidad del SGSI. Por lo tanto, ISO 27001: 2013 no aspira a una evaluación de la continuidad del Negocio tan amplia como la desarrollada al implantar la norma ISO 22301
* 2. ISO 2013 en definitiva Reduce el nivel percibido de garantía de cumplimiento de requisitos de continuidad del negocio proporcionados por el certificado ISO 27001, porque la aclaración deja en claro que ISO 27001 no proporciona garantía amplia en los objetivos de continuidad del negocio.
* 3. Sin embargo para requisitos críticos en materia de Seguridad de la Información, la norma ISO 27001 podrá llegar a niveles aún mayores de exigencia que la norma ISO 22301. (por ejemplo en requisitos para la implantación de sistemas basados en escritorio remoto , aplicaciones y transacciones de datos en la nube (IaaS, PaaS y SaaS)

Veamos una comparativa de requisitos sobre continuidad del Negocio entre ISO 27001:2013 e ISO 27001:2005

* **ISO 27001-2005**
  + A14.OBJETIVOS SOBRE CONTINUIDAD DEL NEGOCIO: Para contrarrestar las interrupciones de las actividades comerciales y para proteger los procesos comerciales críticos de los efectos de las principales fallas de los sistemas de información o desastres y para garantizar su reanudación oportuna.
* **ISO 27001-2013**
  + A17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA CONTINUIDAD DEL NEGOCIO: la seguridad de la información debe estar integrada en los sistemas de gestión de la continuidad del negocio de la organización.
* **ISO 27001-2005**
  + A.14.1.1 – Incluir seguridad de la información en el proceso de gestión de la continuidad del negocio
  + A.14.1.2 – Continuidad del negocio y evaluación del riesgo
  + A.14.1.3 – Desarrollar e implementar planes de continuidad, incluida la seguridad de la información
  + A.14.1.4 – Marco de planificación de la continuidad del negocio
  + A.14.1.5 – Prueba, mantenimiento y reevaluación de los planes de continuidad del negocio
* **ISO 27001-2013**
  + A.17.1.1 – Planificación de la continuidad de la seguridad de la información
  + A.17.1.2 – Implementación de la continuidad de la seguridad de la información A
  + A.17.1.2 – Verificar, revisar y evaluar la continuidad de la seguridad de la información

Veamos los controles y el desarrollo punto por punto de los controles a tener en cuenta en ISO 27001:2013

Citando la norma:

**Objetivo 1:** Continuidad de la seguridad de la información

La continuidad de seguridad del negocio debe estar integrada en los sistemas de gestión de continuidad del negocio de la organización.

* **17.1.1 Planificación de la continuidad de la seguridad de la información**
* **17.1.2 Implementación de la continuidad de seguridad de la información**
* **17.1.3 Verificar, revisar y evaluar la continuidad de la seguridad de la información**

**Objetivo 2:** Redundancia

Garantizar la disponibilidad de las instalaciones de procesamiento de información

* **17.2.1 Disponibilidad de las instalaciones de procesamiento de información**

**OBJETIVO 1: CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN**

La continuidad de seguridad del negocio debe estar integrada en los sistemas de gestión de continuidad del negocio de la organización.

**PLAN DE CONTINUIDAD DEL NEGOCIO y PLANES DE CONTINGENCIA**

Los planes de continuidad van más allá del establecimiento de un plan de contingencias. Los planes de contingencia son una parte de los planes de continuidad donde se establecen las respuestas o tratamiento de las incidencias o contingencias.

Los planes de continuidad contemplan otros aspectos que nos refieren al análisis de las necesidades y riesgos de una organización, la planificación de la respuesta a incidentes y la recuperación ante desastres.

Para ello se establecen los siguientes controles:

**17.1.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN**

En este control se nos pide en primer lugar que verifiquemos que tenemos integrados los requisitos de la seguridad de la información en los planes de continuidad del negocio determinando

* 1. Integrar en los planes de continuidad los requisitos de la seguridad de la información en situaciones de crisis o ante desastres
* 2. En caso de que la organización no cuente con un plan de continuidad formal deberemos tener en cuenta ante una situación de parada de los distintos servicios (energía, comunicaciones, red, colapso de infraestructuras etc.)
  + Un análisis de los requisitos de la seguridad de la información
  + Un análisis de impacto en los requisitos de seguridad de la información (evalué si las necesidades de la seguridad de la información han de mantenerse en el mismo nivel ante situaciones de emergencia)

CASO PRACTICO:  
REQUISITOS DE SEGURIDAD A PROVEEDORES

*Si en nuestro plan de continuidad hemos analizado el impacto de un corte de electricidad y para asegurar el suministro eléctrico hemos contemplado sistemas de soporte como UPS, deberemos realizar una evaluación además de su correcto funcionamiento, de cómo esto afectaría a la seguridad de la información. Para ello deberemos tener en cuenta a modo de ejemplo:*

* *¿El sistema de alimentación alternativo cumple con los requisitos de Seguridad de la Información?*
* *¿Cuánto tiempo puede estar el sistema operando sin fuente de alimentación estable?*
* *¿Cómo afectaría un fallo de más tiempo en la seguridad de la información?*

No debe pasar por alto

*Evite tener que hacer análisis adicionales para el impacto en la seguridad de la información:*

* **Integre los requisitos de la seguridad de la información en la gestión de la continuidad del negocio**
* **Incluya los aspectos de la seguridad de la información en los análisis de impacto en el negocio**
* **Tenga en cuenta la seguridad de la información en los planes de recuperación ante desastres**

**17.1.2 IMPLEMENTACIÓN DE LA CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN**

Se trata de implementar la gestión de la continuidad de la seguridad de la información ante situaciones de emergencia inesperadas

El objetivo será disponer de un plan con medidas concretas para restablecer la disponibilidad de la información en unos plazos identificados mediante unos planes de respuesta ante emergencias que tengan en cuenta la organización y sus recursos

Los principios de la implementación de un plan de continuidad son:

**EL OBJETIVO**

Mantener la Seguridad de la Información ante una emergencia o situación adversa

* **Establecer una Estructura de gestión** que defina
  + Responsabilidades en la continuidad y recuperación de los sistemas
  + Niveles de competencia necesarios en cada función a desempeñar dentro del plan de continuidad
* **Designar a las personas** que van a desempeñar las distintas funciones dentro del plan de continuidad de la seguridad de la información y la recuperación ante desastres.
* **Las funciones de la continuidad** son:
  + Gestionar los incidentes de seguridad de la información
  + Mantener los niveles de seguridad de la información ante emergencias
  + Recuperar los sistemas de información
* **Documentación y procedimientos:** Estas es otra de las funciones de los que forman parte del plan de continuidad de la seguridad de la información aunque la pongamos aparte.

Se trata de un control para que se establezcan procedimientos documentados donde se tenga en cuenta:

* 1. Como se va a gestionar un evento destructivo para la seguridad de la información
* 2. Como se va a mantener la seguridad de la información en un nivel mínimo planificado
* 3. Asegure que se tienen en cuenta los objetivos de la o requisitos mínimos de para la continuidad de la seguridad de la información que hayamos definido en el punto anterior 17.1.1

Importante!

*Veamos en que se traduce todo esto en tres puntos prácticos para implementar la continuidad de la seguridad de la información*

* *1. Considere todos los controles para la seguridad de la información dentro de los planes de continuidad de la Información y de recuperación ante desastres*
* *2. Desarrolle un procedimiento para ver que es necesario o cambiar o implementar dentro de la organización para mantener los controles de seguridad de la información durante situaciones de emergencia*
* *3. Explique cómo va a compensar los controles de seguridad que no puedan ser mantenidos en situaciones de emergencia.*

*En otras palabras, si los controles de seguridad no son capaces de continuar asegurando la información, deberían establecerse controles alternativos para mantener un nivel aceptable de seguridad de la información*

Tenga en cuenta también

*Involucre a los especialistas en Seguridad de la Información en las tareas de continuidad del negocio de forma que apoyen no solo en la aplicación si no la definición de los controles necesarios.*

**17.1.3 VERIFICAR, REVISAR Y EVALUAR LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN**

Las cláusulas de revisión permiten que un sistema se mantenga vivo en el tiempo. Para ello deberemos revisar periódicamente.

* La aplicabilidad de los controles
* El alcance del plan de continuidad en el sentido en que no queden nuevos activos de información fuera del plan de continuidad
* Revisar la implicación del personal en las tareas de recuperación verificando que todo el mundo esté al tanto de sus responsabilidades al respecto

No debe pasar por alto…

*La puesta en marcha de un plan de continuidad del negocio efectivo pasa por atender a este punto con rigurosidad*

Tenga en cuenta que…

*Solo cuando sucede algo que requiere que el Plan de Continuidad del Negocio se ponga en acción es cuando se detectan verdaderamente los problemas.*

*Si a la hora de enfrentar una situación real de la materialización de una amenaza nos damos cuenta que:*

* *No se ha establecido una cadena de mando clara,*
* *La respuesta esperada del equipo de TI no se produce,*
* *Las copias de seguridad no tienen los datos esperados*
* *El personal y los clientes no están seguros de lo que está sucediendo*

*Entonces estamos ante un plan de continuidad que más que ayudarnos causara la ruina de nuestro negocio*

*Un plan de continuidad no tiene porque forzosamente ser algo inasumible en costes y recursos pero puede sin embargo evitar que nuestro negocio naufrague ante la primera dificultad seria a la que nos enfrentemos*

*Un plan de continuidad creado y revisado por expertos de seguro será una herramienta a la que le sacaremos partido*

***Si no tiene un plan de continuidad del negocio, le ayudaremos a crearlo y a probarlo.***

**OBJETIVO 2: REDUNDANCIA**

Garantizar la disponibilidad de las instalaciones de procesamiento de información

Se trata de identificar los activos de información que requieran ser dotados de redundancia atendiendo a la exigencia de los procesos en los que están involucrados

**17.2.1 DISPONIBILIDAD DE LAS INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN**

Como hemos mencionado en la introducción a este objetivo, puede que en nuestra organización tengamos determinados activos de información que requieran una disponibilidad más allá de mantener simples copias de seguridad que requieren de un proceso de recuperación.

En tal caso las exigencias de disponibilidad pueden aconsejar el mantenimiento de sistemas redundantes que nos permitan reaccionar en tiempo real a la caída de sistemas o activos de información estratégicos

En tal caso deberemos realizar los siguientes pasos:

* Identificar que sistemas de información por su arquitectura no pueden garantizar la disponibilidad exigida por los procesos del negocio sin un sistema de respaldo
* Analizar la viabilidad de sistemas redundantes
* Realizar pruebas tanto de buen funcionamiento de los sistemas redundantes como de transición sin interrupciones de un sistema principal a un sistema redundante

**A18 CUMPLIMIENTO**

El último capítulo del anexo A de la norma ISO 27001 está dedicado a controles que nos permitan garantizar el cumplimiento con las políticas, normas y legislación aplicable enfocándose principalmente en lo que se refiere a seguridad de la información.

Citando la norma:

**Objetivo 1:**  
Cumplimiento de los requisitos legales y contractuales

Evitar los incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con los requisitos de seguridad.

* **18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales**
* **18.1.2 Derechos de propiedad intelectual (/PR)**
* **18.1.3 Protección de los registros**
* **18.1.4 Protección de los datos y privacidad de la información personal**
* **18.1.5 Regulación de los controles criptográficos**

**Objetivo.2**  
Revisiones de seguridad de la información

Garantizar que la seguridad de la información es implementada y operada de acuerdo con las políticas y procedimientos organizacionales

* **18.2.1 Revisión independiente de la seguridad de la información**
* **18.2.2 Cumplimiento de la política y las normas de seguridad**
* **18.2.3 Revisión del cumplimiento técnico**

**OBJETIVO 1: CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES**

Hasta ahora hemos visto requisitos para enfrentar el panorama de amenazas para la seguridad de la información con el reto de estar atentos a la constante evolución y las nuevas formas de ataques.

En este punto se nos plantea el reto de cumplir con las leyes, los reglamentos y las obligaciones contractuales requeridas para la seguridad de la información

Esto para muchas organizaciones puede suponer un verdadero reto el enfrentar lo que a veces puede suponer una lista más o menos interminable de regulaciones y requisitos

Sin embargo esto no debe desanimarnos pues el cumplimiento legal puede ser tan importante como los capítulos anteriores

**¿COMO IDENTIFICAMOS LOS REQUISITOS LEGALES?**

Los requisitos obligatorios pueden venir en forma de leyes laborales, requisitos de seguridad relacionados con TI, derechos de propiedad intelectual y leyes de derechos de autor, privacidad, cifrado de datos y leyes de protección;

La pregunta que asusta en este entorno es:

***¿Está tomando todas las medidas necesarias para garantizar que se cumplan las leyes y regulaciones?***

Si Ud. no tiene capacidad de responder ni siquiera a cómo identificar el entorno legal que le afecta entonces:

Nosotros le ayudamos a identificar y cumplir con sus obligaciones legales con relación a la seguridad de la información.

**18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES**

El control establece la necesidad de identificar de forma documentada todos los requisitos legales y contractuales que afecten a la organización, además de mantenerlos actualizados.

Las leyes y reglamentos que afectan a una actividad son algo que evidentemente cambia con el tiempo y pueden ser distintas en cuanto a:

* Leyes o reglamentos sectoriales que afectan a una actividad
* Leyes del parlamento europeo o leyes locales
* Requisitos legales aplicables a tipos de información por su clasificación

En la actualidad dado el crecimiento de los incidentes relacionados con la seguridad y la magnitud de su impacto han hecho que los gobiernos de todo el mundo sean conscientes de la necesidad de proteger a las personas y las empresas contra la gestión inadecuada de la información confidencial.

**18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL (/PR)**

Este control nos requiere que se establezcan procedimientos que garanticen el uso del software de acuerdo a los términos previstos en la Ley de Propiedad Intelectual mencionada en el punto anterior

Para ello se establecen los siguientes puntos a tener en cuenta para cumplir con este control

* ¿Disponemos de una política de uso legal de productos Software?
* ¿Aseguro la no violación de derechos de copia?
  + ¿Dónde compro los productos Software?
  + ¿Mantengo la política de licencias del Software comprado?
  + ¿Controlo el número máximo de usuarios por licencia?
  + ¿Reviso periódicamente que se estén utilizando solamente productos Software con licencia?
  + ¿Cumplo con los derechos de copia de material audiovisual, libros, informes etc.?
* ¿He comunicado al personal la política de uso legal de software aclarando que cosas están permitidas y cuáles no?
* ¿He advertido al personal sobre las consecuencias de la violación de las políticas de uso legal de software estableciendo las medidas disciplinarias oportunas?
* ¿He identificado (listado de activos) los activos de información que están afectados por derechos de propiedad intelectual?
* Finalmente debo mantener la documentación que justifique o acredite la propiedad de las licencias (discos, manuales etc.)

**18.1.3 PROTECCIÓN DE LOS REGISTROS**

Este control nos pide mantener un análisis de los requisitos contractuales legales en cuanto a las obligaciones de debido control sobre la protección de los registros en cuanto a evitar su pérdida, falsificación o acceso no autorizado

***¿De qué registros hablamos?***

Se trata de clasificar los registros de información y aplicar los controles necesarios según los requisitos legales

Por ejemplo:

* Registros contables
* Bases de datos
* Bases de datos de transacciones
* Registros de auditoria (propios del sistema de Gestión de la Seguridad de la información)
* Procedimientos operativos
* Registros documentales en papel, microfichas, archivos electrónicos
* Archivos cifrados (contraseñas, firmas digitales)
* Etc.

Para cumplir con la protección de los registros se nos requiere revisar el cumplimiento con

* La definición y publicación de las directrices sobre la retención, almacenamiento, tratamiento y eliminación de los registros y la información;
* Mantenimiento de un calendario de retenciones donde se identifique los registros y los períodos de tiempo que deberían retenerse;
* Mantenga un inventario de los registros de información clave o critica

**18.1.4 PROTECCIÓN DE LOS DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL**

Este control nos requiere el establecimiento de controles para el cumplimiento de la legislación en materia de cumplimiento con la legislación vigente en materia de protección de datos personales

**18.1.5 REGULACIÓN DE LOS CONTROLES CRIPTOGRÁFICOS**

En caso de utilizar mecanismos de cifrado deben tenerse en cuentas las normativas sobre uso de controles criptográficos vigentes.

**Limitaciones en el uso de medios criptográficos**

En muchos países existen limitaciones en el uso de medios criptográficos por lo que tendremos que tener en cuenta estas limitaciones o restricciones en las importaciones o exportaciones de Hardware y/o Software para funciones criptográficas.

También deberemos considerar si existen métodos obligatorios de cifrado de información y cumplir los requisitos legales del cifrado de información establecidos por los reglamentos de cada país.

**Cifrado Obligatorio**

En el caso de España por ejemplo se tiene en cuenta el reglamento RGPD donde se establece la obligatoriedad de cifrar los datos de carácter personal para los casos siguientes:

Para datos que clasificados como:

* De origen étnico o racial
* Opiniones políticas
* Convicciones religiosas o filosóficas
* Afiliación sindical
* Datos de salud y vidas sexuales
* Datos biométricos
* Uso de datos a gran escala afectados por sistemas de acceso publico

**Códigos de conducta**

Determinadas organizaciones y organismos pueden elaborar códigos de conducta sobre el tratamiento de datos personales.

En este caso si nos adherimos a dichos códigos deberemos cumplir con los requisitos en cuanto al uso y obligatoriedad de los sistemas de cifrado

**EVALUACION DE RIESGOS**

La evaluación de riesgos, también obligatoria en el reglamento RGPD sobre el tratamiento de datos personales puede determinar la necesidad de utilizar cifrado de datos como resultado de un control necesario para mitigar o evitar un riesgo para la seguridad de la información

**CIFRADO LEGAL: REQUISITOS**

En el caso que nos veamos obligados a cifrar datos según lo expuesto hasta ahora deberemos dedicar los recursos necesarios para cumplir con estos requisitos.

Cualquier sistema de cifrado no es suficiente.

Por ejemplo los archivos PDF o archivos comprimidos ZIP con clave no son considerados válidos para garantizar que la información no sea inteligible ni manipulada por terceros.

**OBJETIVO.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN**

Garantizar que la seguridad de la información es implementada y operada de acuerdo con las políticas y procedimientos organizacionales.

La revisión de que las políticas de seguridad y procedimientos para la seguridad de la información se cumplen es un requisito fundamental dentro de la norma ISO 27001 como ya hemos visto.

Para ello se establecen los siguientes controles.

**18.2.1 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN**

¿Quién debe llevar a cabo las revisiones de cumplimiento de la seguridad de la información?

Las revisiones deben ser llevadas a cabo por personal independiente al personal que es auditado . Aunque pueden ser llevadas a cabo por personal interno siempre de áreas o departamentos independientes al auditado, conviene que de forma regular se realicen auditorias de cumplimiento de la seguridad de la información por personal externo.

Las auditorías realizadas por personal externo siempre podrán aportar beneficios como:

* Garantizar la independencia de las revisiones o auditorias
* Aportar un punto de vista imparcial
* Aportar la experiencia de profesionales de la seguridad de la información que conocen otras organizaciones y pueden aportar mejoras.

**18.2.2 CUMPLIMIENTO DE LA POLÍTICA Y LAS NORMAS DE SEGURIDAD**

Este control nos pone como requisito la necesidad de que los responsables de cada área deben revisar que los procedimientos de la organización sean aplicados de acuerdo a los requisitos definidos

Para ello los responsables deberían:

* Determinar la forma de revisar cómo se cumplen los requisitos de seguridad de la información definidos en las políticas, normas y en otras regulaciones aplicables.
* Tener en cuenta la implementación de sistemas de medición automática y herramientas de informes

Cuando se identifican incumplimientos se deberá:

* Identificar las causas
* Evaluar la necesidad de tomar medidas
* Implementar las acciones correctivas apropiadas;
* Revisar la eficacia de las acciones correctivas
* Identificar las deficiencias y debilidades del sistema

***NOTA:****Se deben mantener registros documentados de los resultados de las revisiones y de las acciones correctivas realizadas para poder realizar informes con los resultados*

**18.2.3 REVISIÓN DEL CUMPLIMIENTO TÉCNICO**

Para la evaluación de los sistemas de información debe revisarse periódicamente si están configurados correctamente de acuerdo a las reglas y políticas definidas

El objetivo es:

* Identificar fallos en las actualizaciones de los sistemas
* Establecer medidas correctivas antes de que estos fallos puedan suponer una amenaza real para el sistema