

CENTRO DE EXCELENCIA DE SOFTWARE LIBRE DE CASTILLA-LA MANCHA

JUNTA DE COMUNIDADES DE CASTILLA LA MANCHA.



RECOMENDACIONES PARA EL DESARROLLO DE UNA PLAN DE SEGURIDAD DE LA INFORMACIÓN



Autor del documento:

Centro de Excelencia de Software Libre de Castilla-la Mancha de la Fundación Parque Científico y Tecnológico de Albacete

Datos de contacto:

E-Mail: ceslcam@ceslcam.com

Página Web: www.ceslcam.com

Teléfono: 967 555 311

Versión del documento:

1.0

Fecha: 20-07-2011

Licencia del documento:

CopyRight © 2011, Junta de Comunidades de Castilla-La Mancha

Publicado bajo licencia Creative Commons By - Sa

Usted es libre de:

- Copiar, distribuir y comunicar públicamente la obra.
- Hacer obras derivadas

Bajo las condiciones siguientes:

- Reconocimiento. Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciador (pero no de una manera que sugiera que tiene su apoyo o apoyan el uso que hace de su obra).
- Compartir bajo la misma licencia. Si transforma o modifica esta obra para crear una obra derivada, sólo puede distribuir la obra resultante bajo la misma licencia, una similar o una compatible.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.

Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor.

Nada en esta licencia menoscaba o restringe los derechos morales del autor.

Índice de contenido

1	Contexto.....	4
2	Política de Gestión de la Seguridad de la Información.....	5
2.1	Gestión de los Activos.....	7
2.2	Seguridad Ligada a los Recursos Humanos.....	8
2.3	Seguridad Física y Ambiental.....	9
2.4	Gestión de las Comunicaciones y Operaciones.....	10
2.5	Control de Acceso Lógico.....	12
2.6	Gestión de Incidencias de Seguridad.....	14
2.7	Planes de Contingencia.....	15
2.8	Cumplimiento Requisitos Legales.....	17
3	Otras recomendaciones.....	18

1 Contexto

Este documento presenta algunas recomendaciones generales para ayudar a definir la política y procedimientos adecuados para la gestión de la seguridad de la información de los sistemas de una empresa.

El objetivo de la definición de este documentos es establecer las actividades y protocolos que deben ejecutarse para asegurar la confidencialidad, integridad y disponibilidades de los sistemas de información de la empresa.

El presente documento, al ser un modelo genérico, debe tenerse únicamente como referencia, debiendo ser adaptado a la particularidad y necesidad de cada empresa. Por tanto, los elementos descritos en el documento deben considerarse como una referencia no estricta.

Si se desea obtener un asesoramiento más personalizado se recomienda contactar directamente con el Centro de Excelencia de Software Libre de Castilla-La Mancha.

Para la redacción de este documento se ha seguido las principales recomendaciones realizadas en el marco de la norma ISO 27001.

2 Política de Gestión de la Seguridad de la Información

La Política de Seguridad de la Información tiene como objetivo establecer las normas y requisitos de seguridad que permitan garantizar la confidencialidad, integridad y disponibilidad de los sistemas de información de la empresa.

La Política de Seguridad de la Información es un documento que denota el compromiso de la gerencia con la seguridad de la información y debe contener la definición de la seguridad de la información bajo el punto de vista de la entidad.

Los aspectos más importantes a tener en cuenta en la Política de Seguridad son:

- Garantizar la confidencialidad, integridad y disponibilidad de los sistemas de información de la empresa
- Disponer de un responsable de seguridad encargado de la gestión de la seguridad de la empresa.
- Cumplir los requisitos legales que sean aplicables en la empresa.
- Gestionar las incidencias de seguridad de forma adecuada.
- Disponer de un plan de contingencia que permita a la empresa recuperarse en caso de desastre o discontinuidad de los sistemas.
- Informar a los empleados de sus obligaciones con respecto a la seguridad de los sistemas, sus obligaciones y los procedimientos definidos que les afectan
- Formar a los empleados en los principales conceptos de la gestión de la seguridad de los sistemas.

La Política de Seguridad está sustentada por el Manual de Seguridad que incluye un conjunto de normas de seguridad y procedimientos. Este manual ¹ puede estructurarse de diversas formas. Una de las propuestas más habituales es la utilizada en las certificaciones ISO 27001:

- Gestión de los activos.
- Seguridad ligada a los recursos humanos.
- Seguridad física y ambiental.
- Gestión de la comunicaciones y operaciones.
- Control de acceso lógico.
- Gestión de incidentes.
- Planes de contingencia
- Cumplimiento de requisitos legales

¹ La Política de Seguridad debe recoger entre otros elementos una visión general del manual de seguridad de la empresa.

La Política de Seguridad debe ser:

- Compatibilizada con otras políticas dependientes de ésta, objetivos de seguridad, normas de seguridad y procedimientos. Puede ser también un documento único o embebido en un manual de seguridad.
- Asignada a un propietario que será el responsable de su mantenimiento y su actualización a cualquier cambio que se requiera .
- Conocida y entendida por todos los empleados de la empresa².

Aunque en los próximos epígrafes se incluye información más detalladas sobre los procedimientos a implementar en el ámbito de la gestión de la seguridad, los elementos que no pueden olvidarse son los siguientes ³:

- **Gestión de las Comunicaciones y Operaciones.**
- **Gestión del Acceso Lógico.**
- **Gestión de la Continuidad.**

A continuación se detallan los procedimientos que debe recoger el Manual de Seguridad.

2 No olvidar nunca que la política tiene que ser conocida por los empleados. Estos también deben conocer sus responsabilidades en la gestión de la seguridad dentro de su entorno de trabajo, especialmente en la protección de los activos de los que son propietarios, contraseñas de acceso a los sistemas y la documentación en uso.

3 Algunos de los elementos que influyen en la definición de una Política de Gestión de la Información más exhaustiva son: el nº de empleados, el perfil de estos, la criticidad de la información gestionada y el grado de implantación TIC.

2.1 Gestión de los Activos

El objetivo de la Gestión de Activos es asegurar que todos los activos de la empresa se encuentran identificados y reciben el nivel de protección adecuado.

Dentro de este procedimiento es necesario definir:

- Inventario de los Activos y asignación de propietario/responsable.
- Clasificación de los Activos, según su valor, los aspectos legales o criticidad para la empresa.
- Roles que intervienen en el proceso
- Responsabilidades de los roles.
- Definición del procedimientos de gestión y uso según la clasificación definida:
 - Criterios para la clasificación.
 - Etiquetado.
 - Acceso a los Activos.
 - Almacenamiento.
 - Difusión.
 - Trasmisión o Transporte.
 - Destrucción.
- Documentación y registros a generar ⁴.
- Documentación y plantillas de referencia.

A la hora de definir y gestionar los Activos es de utilidad tener en cuenta los siguientes principios:

- La información debe estar clasificada según su valor, los requisitos legales, su sensibilidad y criticidad para la organización. Habitualmente se clasifica como: público, interno o confidencial.
- Se considera información a todo dato relacionado con las actividades y servicios de la organización, que tenga valor para ésta según estime su propietario, atendiendo a las escalas de valoración utilizadas, los requisitos legales, su sensibilidad y criticidad para la organización, cualquiera que sea su forma y medio de comunicación y/o conservación.
- Toda información definida como activo debe ser clasificada para garantizar un nivel adecuado de protección.
- Los soportes (CD, papel, Discos Duros,...) que contengan información de distintos niveles de clasificación serán clasificados con el nivel más alto de los activos de información que contengan.
- Los propietarios de los activos son responsables de conocer los niveles de clasificación de información establecidos por la organización y garantizar el cumplimiento de las normas de protección. Con dicha finalidad la organización debe distribuir una Política de uso en la que se describan los niveles de clasificación y el proceso de etiquetado.

⁴ Especialmente importante el seguimiento del estado de los activos.

2.2 Seguridad Ligada a los Recursos Humanos

El objetivo de este procedimiento es asegurar que todo el personal interno y externo⁵ conoce y aplica las medidas de seguridad establecidas por la empresa.

Dentro de este procedimiento es necesario definir:

- Escenarios posibles (antes, durante y después de la contratación) y actividades a realizar.
- Perfiles de usuario para cada área de la empresa con respecto a la seguridad.
- Roles que intervienen en el proceso.
- Responsabilidades de los roles.
- Documentación y registros a generar.
- Documentación y plantillas de referencia.

La seguridad ligada a los recursos humanos se gestionará a tres niveles:

1. Antes de la contratación.

Los responsables de cada área junto con la Dirección de la organización deben definir los perfiles de cualificación que definen las funciones y responsabilidades de seguridad de la organización, adecuados a los requisitos del puesto a ocupar, en los que se especificará las competencias que deben cubrir las personas que ocupen el puesto de trabajo en cuestión.

La selección de personal se realizará siguiendo estos perfiles e informando de las obligaciones y responsabilidades al empleado, junto a los términos y condiciones de contratación.

2. Durante la contratación.

Durante la vida laboral, todo el personal de la entidad deberá recibir una formación y concienciación adecuadas y actualizadas de las políticas y procedimientos de seguridad, adaptadas según el puesto de trabajo y las necesidades de seguridad que vayan siendo detectadas por parte de los responsables del área al que pertenezca el empleado.

La formación debe incluir requisitos de seguridad, responsabilidades legales y controles de negocio, así como formación en el uso correcto de los recursos de tratamiento de la información.

3. Tras finalizar la contratación o el cambio de puesto de trabajo.

En los casos relacionados con el cese del puesto de trabajo, todos los empleados, contratistas y externos deben devolver todos los activos (componentes software, documentos corporativos y equipos prestados) de la organización que tengan en su posesión y estén relacionados con su empleo. Asimismo, se deberán revocar todos los privilegios al usuario cesado en todos los entornos de producción o accesibles desde el exterior de la organización.

En los casos relacionados con el cambio de puesto de trabajo dentro de la organización el Administrador del Sistema deberá revocados todos los privilegios excesivos que el usuario tuviera en el puesto actual respecto al nuevo puesto a desempeñar.

⁵ Personas externas a la empresa que participan en los procesos de la empresa.

2.3 Seguridad Física y Ambiental

El objetivo de este procedimiento es proteger los recursos de tratamiento de la información crítica y sensible de la organización, a través de áreas restringidas y perímetros de seguridad definidos mediante adecuadas barreras de seguridad y controles de entrada.

Dentro de este procedimiento es necesario definir:

- Elementos físicos y ambientales a proteger.
- Medidas de protección.
- Roles que intervienen en el proceso.
- Responsabilidades de los roles.
- Elementos a proteger.
- Medidas de protección.
- Documentación y registros a generar.
- Documentación y plantillas de referencia.

Dentro de las medidas principales a realizar para protección de los elementos físicos se encuentran:

- **Áreas Seguras.**

Prevenir los accesos físicos no autorizados, los daños y las interferencias a las instalaciones de la organización y a la información: accesos sólidos y protegidos a las instalaciones, detección de condiciones ambientales adversas (fuego principalmente), detección de accesos no autorizados (alarmas, sensores de movimientos, cámaras...), medidas de protección de accesos (llaves, tarjetas, lectores de huella...) e información física, etc.

- Definición de Áreas de Trabajo.

En función de la finalidad a la que se destinan los espacios o áreas de trabajo, se pueden establecer los siguientes tipos de áreas: públicas, internas, restringidas, etc.

- Activos de Información.

Debe asegurarse la protección de los activos de la empresa, especialmente los de información: protegiendo los soportes extraíbles, los armarios y cajoneras, no dejando accesible ningún tipo de información clasificada como interna o confidencial, etc.⁶

- **Protección de los Sistemas.**

Prevenir la pérdida, daño, robo o el compromiso de los activos y la interrupción de las actividades de la organización: áreas seguras para servidores de aplicaciones, datos y redes, sistemas SAI para los sistemas clave de la empresa, protección de los sistemas o soportes a extraer fuera de la organización, destrucción de los datos incluidos en soportes a desechar, etiquetado y documentado de equipos y cables, etc.

⁶ En el control de los activos públicos influye particularmente la gestión que de ellos hagan los empleados por lo que es muy importante inculcar la importancia de protegerlos, asegurarse de no dejar información al acceso de terceras personas en su mesa (documentos, pendrives, ...), bloquear acceso al sistema operativo, dejar ordenadores portátiles encima de la mesa sin protección, cerrar cajoneras, puertas, cerrar ventanas, etc.

2.4 Gestión de las Comunicaciones y Operaciones

El objetivo de este procedimiento es establecer las responsabilidades y procedimientos para la gestión y operación de todos los recursos de información.

Dentro de este procedimiento es necesario definir:

- Tareas a realizar y periodicidad de las tareas.
- Roles que intervienen en el proceso.
- Responsabilidades de los roles.
- Normas de uso de los recursos lógicos de la empresa.
- Documentación y registros a generar.
- Documentación y plantillas de referencia.

Las áreas prioritarias que deben gestionarse dentro de este procedimiento son:

- **Actualización de los sistemas.**

Es clave la correcta gestión de las actualizaciones de los sistemas críticos de la empresa para asegurar su disponibilidad. Son especialmente sensibles a estos cambios son: servidores, aplicaciones de gestión, bases de datos, firewall, redes, etc.

- **Protección de los sistemas frente a código malicioso o descargable.**

Es clave proteger los sistemas frente a este tipo de ataques para asegurar su confidencialidad/integridad. Para ello se recurrirá a herramientas antivirus y actualizaciones de los sistemas ⁷.

- **Seguridad de las redes.**

Es clave proteger las redes y comunicaciones de la organización para asegurar la confidencialidad/integridad/disponibilidad de los datos y sistemas de la empresa. Para ello es necesario implantar algún sistema cortafuegos y definir correctamente las reglas de acceso tanto de entrada como de salida a los sistemas, denegando por defecto todo lo que no esté explícitamente permitido.

Especial atención hay que tener en los accesos desde el exterior a los servicios y servidores de la empresa. En caso que sea necesario acceder desde el exterior a estos servicios por un trabajador deben definirse VPN e incluso controlar los equipos a través de reglas que equipos concretos pueden conectarse.

Es recomendable a su vez:

- Realizar revisiones periódicas del material disponible: firewall, enrutadores, conmutadores, cableado, etc.
- Activar y revisar el visor de sucesos de los sistemas críticos de la empresa de forma periódica. Para facilitar esta tarea es posible utilizar herramientas para monitorización de

⁷ Aunque se utilicen sistemas GNU/Linux también es recomendable disponer de sistemas antivirus, pues aunque este tipo de software no suele afectarles, podría propagarse a otros sistemas de clientes o de empleados fuera de la oficina.

los sistemas o generar scripts para extraer información resumida de los logs de sistema.

- **Registro de actividades.**

Al igual que la monitorización de los sistemas críticos de la empresa puede ser necesario monitorizar el resto de recursos de la empresa: uso de la red, aplicaciones instaladas, inicio y fin de las sesiones de trabajo, acceso y/o modificación de información crítica, etc.

En caso de registrar actividades relacionados de los trabajadores de la empresa es necesario que estos estén informados de forma explícita del uso que puede hacerse de los recursos de la empresa y que la actividad podrá ser monitorizada por la empresa.

- **Copias de seguridad.**

Es clave la correcta gestión de las copias de seguridad de la organización para poder asegurar la integridad/disponibilidad de los datos y los sistemas de la empresa. Es necesario definir el qué (elementos a respaldar), el cuándo (con que frecuencia se realizará), el dónde (lugar de almacenamiento) y el cómo (proceso para realizar el respaldo).

Los puntos claves del procedimiento de copias de seguridad deben responder a dichas preguntas, asegurando que:

- Los datos y sistemas claves de la organización están protegidos: documentos, bases de datos, configuraciones de servidores y servicios, imágenes de sistemas operativos y servidores, ...
- Se haga con la suficiente periodicidad, teniendo en cuenta esfuerzo vs riesgo. Algunos datos se copiarán diariamente, otros semanalmente y quizá otros mensual o semestralmente.
- Se almacenen las copias en lugar seguro. Es habitual que existan al menos dos niveles de copia. Una dentro de las oficinas de la empresa y otra fuera de la oficina.
- A la hora de realizar las copias hay diversas maneras de hacerlo, cada una con sus pros y contras. Es necesario que la empresa defina el tipo de copia de seguridad que se realizará. Pueden ser incrementales, completas, automatizadas o manuales, también puede realizarse una copia de los datos mediante herramientas de sincronización que solo realiza la copia cuando el fichero ha sido modificado en origen.
- Es necesario verificar que las copias finalizan correctamente y realizar pruebas de restauración periódicas para verificar que el sistema de respaldo funciona correctamente.

Existen diversas aplicaciones software libre para automatizar los backups: rsync, bacula, amanda, etc.

2.5 Control de Acceso Lógico

El objetivo de este procedimientos es proteger los sistemas lógicos de la empresa para asegurarse que solo los usuarios definidos tenga acceso lógico a los datos y sistemas.

Todos los sistemas de la empresa dispondrán de un sistema de autenticación de los usuarios, de forma general será a través de usuario y contraseña. Si bien pueden implantarse otros sistemas como son el uso de certificados digitales o tarjetas inteligentes, lectores de huella, etc

Dentro de este procedimiento es necesario definir:

- Niveles de control de acceso
- Medidas de protección a implantar y tareas a realizar.
- Roles que intervienen en el proceso.
- Responsabilidades de los roles.
- Normas de acceso lógico a los recursos de la empresa.
- Normas para la creación y gestión de contraseñas ⁸.
- Documentación y registros a generar ⁹.
- Documentación y plantillas de referencia.

Entre las actividades principales a realizar dentro de este procedimiento destacan:

- **Definición de los niveles de acceso.**

Los niveles de acceso lógico a los sistemas suelen ser habitualmente tres: red, sistema operativo y aplicación/datos.

Para cada uno de los niveles es necesario definir explícitamente, especialmente a nivel de red ¹⁰, los recursos que serán controlados.

- **Definición de las medidas técnicas a implantar.**

Existen diversas medidas para controlar los accesos, la mayor parte de ellas a través de algún tipo de sistema de autenticación ¹¹: ip/mac, usuario y contraseña, certificado o tarjeta inteligente, huella dactilar, token de seguridad, etc.

A nivel de red existen otro tipo de medidas más allá de la autenticación, como puede ser la segregación de redes, filtrado de conexiones, enrutamiento, etc.

- **Definición de los permisos de acceso.**

La definición de los permisos de usuarios debe hacerse mediante roles o grupos, asignando a cada rol o grupo un conjunto de permisos sobre el acceso lógico a los sistemas; cada usuario

8 Especialmente importante es la correcta gestión de las contraseñas: tipo de contraseñas aceptadas, validez temporal, almacenamiento, etc.

9 Especialmente importante es el registro de los usuarios de los sistemas de información de la empresa e identificación de los privilegios de estos usuarios.

10 Servicios web, correo electrónico, servicios de charla y mensajería instantánea, transferencia de ficheros, acceso interactivo a equipos remotos, acceso a aplicaciones remotas, acceso a redes de intercambios de ficheros P2P

11 Puede ser interesante implantar un sistema centralizado de autenticación por ejemplo a través de ldap.

estará asignado a un rol o grupo. Es recomendable seguir una política de “mínimo privilegio” (need to know), en función de las necesidades de cada puesto de trabajo.

- **Definición y difusión de políticas de acceso.**

Algunas de las políticas básicas que deben definirse son la gestión de contraseñas y las políticas de acceso a datos. Estas políticas deben ser conocidas explícitamente por los empleados.

También es habitual que se definan las sanciones por el incumplimiento de estas políticas.

A la hora de implantar los niveles de acceso, como ya se ha indicado, se contempla:

- **Acceso a nivel de Red.**

Se debe controlar el acceso a los servicios en red, tanto internos (red local) como externos (internet). La empresa debe establecer las políticas que controlen el uso del entorno de red (correo electrónico, navegación web, DNS, etc.), así como las políticas de filtrado de conexiones en los equipos de seguridad perimetral (firewalls).

- **Acceso a nivel de sistema operativo.**

Segundo nivel de control de acceso que permite a los empleados utilizar los sistemas operativos de la red.

- **Acceso a nivel de aplicaciones y datos.**

Tercer nivel en el control de acceso al sistema de información de GRUPO AMIAB. Se debe definir una política de control de acceso de los usuarios para prevenir el acceso no autorizado a la información y a las aplicaciones.

En cuanto a la política de contraseñas los principales elementos a tener en cuenta para su correcta gestión son:

- Contraseñas fuertes: más de 6 u 8 caracteres, incluir números, letras, números y caracteres no habituales.
- Renovación periódica de las contraseñas.
- No revelación de las contraseñas.
- Bloqueo de los equipo cuando no vayan a ser usado.
- Almacenamiento seguro. No escribir las contraseñas en post-it o papel, no almacenar en los navegadores, no revelar nunca las contraseña a otro usuario, etc En este caso la mejor opción es utilizar una herramienta de gestión de contraseñas.

2.6 Gestión de Incidencias de Seguridad

El objetivo de la Gestión de Incidencias es resolver de la manera más rápida y eficaz posible, cualquier incidente o no conformidad relacionada con la seguridad de los sistemas.

Dentro del procedimiento es necesario definir:

- Fases y actividades a realizar para la gestión de Incidencias. Flujo básico de una incidencia: Registro, Clasificación, Diagnóstico y Resolución.
- Roles que intervienen en el proceso
- Responsabilidades de los roles.
- Sistema de clasificación de incidencias: niveles de incidencias y criticidad.
- Estructura del registro de incidencias: campos para documentar la incidencia.
- Documentación y registros a generar.
- Documentación y plantillas de referencia.

Este procedimiento puede estar integrado dentro del procedimiento general de gestión de incidencias implantado en la empresa.

Debe existir un teléfono de emergencia o persona de contacto para la atención de incidencias que se utilizará siempre que los canales habituales dejen de estar operativos.

A continuación se incluyen algunos ejemplos de incidencias de seguridad:

- Pérdida de servicio, equipos o instalaciones
- Fallos o sobrecargas del sistema
- Incumplimiento de políticas o directrices
- Incumplimientos de los acuerdos de seguridad física
- Cambios del sistema no controlados
- Fallos del software o del hardware
- Violaciones de acceso
- Eventos que afecten a la identificación y autenticación de los usuarios
- Eventos que afecten a los derechos de acceso a los datos
- Eventos que afecten a los procedimientos de copias de seguridad y recuperación.
- Incidencias que afecten a la gestión de soportes

2.7 Planes de Contingencia

El objetivo del Plan de Contingencia es reaccionar a la interrupción de las actividades empresariales y proteger los procesos críticos de negocio de los efectos de desastres o de fallos importantes de los sistemas de información, así como garantizar su oportuna reanudación.

Dentro de este procedimiento es necesario definir:

- Desarrollo de planes de contingencia
- Establecimiento del Marco de Referencia de los Planes de Contingencia.
- Roles que intervienen en el proceso.
- Responsabilidades de los roles.
- Documentación y registros a generar ¹².
- Documentación y plantillas de referencia.

Para poder desarrollar planes de contingencia adecuados a la empresa es necesario:

- **Analizar la organización.**

El objetivo de esta fase es conocer las actividades, activos y recursos claves para la organización y los clientes. Analizar el impacto en el negocio de una interrupción de los procesos de negocio. Identificar los riesgos, probabilidad de ocurrencia e impacto.

Con la información recopilada es posible determinar las estrategias de continuidad.

- **Determinar las estrategias de continuidad.**

A la hora de definir las estrategias de continuidad tendrá que tenerse en cuenta, para cada proceso, el periodo máximo tolerable de interrupción, el coste de implementar las medidas y las consecuencias de no llevar a cabo ninguna acción.

Se recomienda definir las estrategias según el recurso:

- Personas. Documentar los conocimientos críticos para la empresa, disponer al menos dos personas con los conocimientos suficientes para gestionar un proceso/área, segregar responsabilidades para evitar que todo el conocimiento recaída sobre una única persona, etc.
- Locales. Planificar la posibilidad de trabajar desde otros lugares en caso que no puede accederse a las instalaciones. Por ejemplo, disponiendo de locales alternativos o trabajando de forma remota.
- Tecnología. Implantar las medidas necesarias que permitan mitigar la discontinuidad de los sistemas: sistemas de backups (aplicaciones, datos, servidores...), redundancia de los sistemas (redes, servidores, datos...), etc.
- Información. Implantar sistemas de recuperación de información: sistemas de backup, recuperación de disco, etc.

¹² Especialmente importante es el registro de los usuarios de los sistemas de información de la empresa e identificación de los privilegios de estos usuarios.

- Suministros. En este caso es necesario disponer de un inventario de los suministros críticos para la continuidad de negocio y estrategias para suplir la discontinuidad: acuerdos de entrega, almacenaje de suministros adicionales, proveedores alternativos, ...

- **Desarrollo de protocolos de recuperación.**

En esta fase se desarrollarán e implantarán los planes para garantizar la continuidad de actividades críticas y la gestión de incidentes. Todos los planes deben contener al menos la siguiente información:

- Actividades críticas que deben ser recuperadas y bajo que situaciones debe aplicarse el plan.
- Actividades críticas priorizadas y enmarcadas por los periodos de tiempo, y niveles de recuperación necesarios.
- Roles y responsabilidades durante el incidente.
- Procedimientos para la activación de la gestión de incidentes, continuidad del negocio o recuperación.
- Responsable de la actualización de cada plan.
- Datos de contacto de las personas clave implicadas en cada plan.

El Marco de Referencia de los Planes de Contingencia recogerá una visión estandarizada de todos los planes de contingencia incluyendo la información crítica:

- Protocolo de activación del plan de contingencia.
- Responsables de la gestión de la recuperación.
- Actividades a realizar para recuperar el sistema.
- Información de referencia.

Por último, recordar que es necesario que el Marco de Referencia sea conocido explícitamente por los empleados de la empresa.

2.8 Cumplimiento Requisitos Legales

El objetivo de este procedimientos es identificar los requisitos legales, reglamentarios y contractuales de seguridad a los que están sujetos los sistemas de información.

Dentro del procedimiento es necesario definir:

- Requisitos legales a cumplir.
- Tareas a realizar para cumplir los requisitos legales
- Roles que intervienen en el proceso
- Responsabilidades de los roles.
- Documentación y registros a generar.
- Documentación y plantillas de referencia.

Los principales requisitos legales en el marco de la regulación española son:

- Derechos de propiedad intelectual.
- Protección de los registros y privacidad de la información personal (LOPD).

3 Otras recomendaciones

Para finalizar esta guía, se recogen a continuación una serie de puntos claves para definir un procedimiento genérico. Estos puntos deben ser:

- Incluir información sobre la fecha de realización, versión del documento y control del historial.
- Definición del objetivo del procedimiento. Incluye una descripción clara y breve del propósito o propósitos del procedimiento.
- Definición del alcance del procedimiento. Incluye información de dónde y bajo qué circunstancias se aplicará el procedimiento
- Terminología y definiciones. Incluye las descripciones de aquellos términos técnicos, de calidad y/o administrativos que deben ser explicados, así como las definiciones que son utilizadas en la aplicación del procedimiento.
- Responsabilidades. Incluye definición de los roles participantes en el proceso y responsabilidades/actividades prioritarias de cada rol.
- Documentación de Referencia. Incluye una relación de documentos tales como normas, procedimientos, manuales y métodos que son necesarios para la elaboración del procedimiento en cuestión.
- Elementos de entrada al procedimiento. Incluye cualquier elemento que se utiliza dentro del procedimiento y que no haya sido generado internamente en dicho procedimiento.
- Registros de calidad y elementos de salida. Incluye cualquier elemento que se genere o se modifique durante el procedimiento junto a los registros que deben ser mantenidos para dejar evidencia del cumplimiento del seguimiento del procedimiento.
- Descripción del procedimiento. Incluye información breve y concisa de todos los pasos a seguir para la ejecución del procedimiento. Cuando sea necesario se deberán incluir un diagrama de flujo para el mayor entendimiento del procedimiento. La descripción del procedimiento incluirá información de las actividades o fases en que se divide el procedimiento y de las subtarear a realizar en cada actividad o fase.

En caso que alguno de estos conceptos no tengan descripción, por no ser necesario o que no exista, se debe incluir la leyenda “No aplica”.

En la redacción de los procedimientos se pueden utilizar las siguientes formas para determinar una o varias situaciones:

- “Debe”, implica modo imperativo, ejemplo: debe ser, debe realizar, debe llevarse a cabo.
- “Puede”, implica la opción de tomar una o varias alternativas, ejemplo: puede ayudarse de gráficas o diagramas de flujo, puede capacitarse por cualquiera de los siguientes métodos, etc.