[logo de la organización]

[nombre de la organización]

Comment [DK1]: Se deben completar todos los campos de este documento que estén marcados con corchetes [ ].

# POLÍTICA DE USO ACEPTABLE

| | |
|---|---|
| Código | |
| Versión: | |
| Fecha de la versión: | |
| Creado por: | |
| Aprobado por: | |
| Nivel de confidencialidad: | |

Comment [DK2]: El sistema de codificación del documento debe coincidir con el sistema actual de codificación de documentos de la organización. En el caso que no exista ese sistema, se puede eliminar esta línea.

©2013 Plantilla para clientes de EPPS services Ltd. www.iso27001standard.com, según Contrato de licencia.

## Historial de modificaciones

| Fecha | Versión | Creado por | Descripción de la modificación |
|---|---|---|---|
| 10/01/2013 | 0.1 | Dejan Kosutic | Descripción básica del documento |
| | | | |
| | | | |
| | | | |
| | | | |

## Tabla de contenido


**1. OBJETIVO, ALCANCE Y USUARIOS ..... 3**

**2. DOCUMENTOS DE REFERENCIA ..... 3**

**3. USO ACEPTABLE DE LOS ACTIVOS DE INFORMACIÓN ..... 3**

3.1. DEFINICIONES ..... 3
3.2. USO ACEPTABLE ..... 3
3.3. RESPONSABILIDAD SOBRE LOS ACTIVOS ..... 3
3.4. ACTIVIDADES PROHIBIDAS ..... 4
3.5. USO DE ACTIVOS FUERA DE LAS INSTALACIONES ..... 4
3.6. DEVOLUCIÓN DE ACTIVOS A LA FINALIZACIÓN DE UN CONTRATO ..... 4
3.7. PROCEDIMIENTO PARA COPIAS DE SEGURIDAD ..... 4
3.8. PROTECCIÓN ANTIVIRUS ..... 4
3.9. FACULTADOS PARA EL USO DE SISTEMAS DE INFORMACIÓN ..... 4
3.10. RESPONSABILIDADES SOBRE LA CUENTA DE USUARIO ..... 5
3.11. RESPONSABILIDADES SOBRE LA CLAVE ..... 5
3.12. POLÍTICA DE PANTALLA Y ESCRITORIO LIMPIO ..... 5
*3.12.1. Política de escritorio limpio ..... 5*
*3.12.2. Política de pantalla limpia ..... 6*
*3.12.3. Protección de instalaciones y equipos compartidos ..... 6*
3.13. USO DE INTERNET ..... 6
3.14. CORREO ELECTRÓNICO Y OTROS MÉTODOS DE INTERCAMBIO DE MENSAJES ..... 7
3.15. DERECHOS DE AUTOR ..... 7
3.16. COMPUTACIÓN MÓVIL ..... 7
*3.16.1. Introducción ..... 7*
*3.16.2. Reglas básicas ..... 8*
3.17. TELE-TRABAJO ..... 8
3.18. SUPERVISIÓN DEL USO DE SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN ..... 9
3.19. INCIDENTES ..... 9

**4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO ..... 9**

**5. VALIDEZ Y GESTIÓN DE DOCUMENTOS ..... 11**




©2013 Plantilla para clientes de EPPS services Ltd. www.iso27001standard.com, según Contrato de licencia.

## 1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir reglas claras para el uso de los sistemas y de otros activos de información en [nombre de la organización].

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los sistemas y demás activos de información utilizados dentro del alcance del SGSI.

Los usuarios de este documento son todos los empleados de [nombre de la organización].

## 2. Documentos de referencia

- Norma ISO/IEC 27001, capítulos A.6.2.1, A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.9.3.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3, A.18.1.2
- Política de Seguridad de la Información
- [Política de Clasificación de la Información]
- [Procedimiento para gestión de incidentes]
- [Inventario de activos]
- [Procedimientos operativos para tecnología de la información y de la comunicación]
- [Política de Transferencia de la Información]

## 3. Uso aceptable de los activos de información

**Comment [DK3]:** En base a los resultados de la evaluación de riesgos se debe determinar hasta dónde es necesario cada punto enumerado.

### 3.1. Definiciones

Sistema de información: incluye todos los servidores y clientes, infraestructura de red, software del sistema y aplicaciones, datos y demás subsistemas y componentes que pertenecen o son utilizados por la organización, o que se encuentran bajo responsabilidad de la organización. El uso de un sistema de información también incluye el uso de todos los servicios internos o externos, como el acceso a Internet, correo electrónico, etc.

Activos de información: en el contexto de esta Política, el término activos de información se aplica a los sistemas de información y demás información o equipos, incluyendo documentos en papel, teléfonos móviles, ordenadores portátiles, soportes de almacenamiento de datos, etc.

### 3.2. Uso aceptable

Los activos de información solamente pueden ser utilizados a fines de satisfacer necesidades de negocios con el objetivo de ejecutar tareas vinculadas con la organización.

### 3.3. Responsabilidad sobre los activos

**Comment [DK4]:** Eliminar todo este punto si el control A.8.1.2 está marcado como no aplicable en la Declaración de aplicabilidad.

Cada activo de información tiene designado un propietario en el Inventario de activos. El propietario del activo es el responsable de la confidencialidad, integridad y disponibilidad de la información en el activo en cuestión.



©2013 Plantilla para clientes de EPPS services Ltd. www.iso27001standard.com, según Contrato de licencia.

### 3.4. Actividades prohibidas

Está prohibido utilizar los activos de información de manera tal que ocupen innecesariamente capacidad, que disminuya el rendimiento del sistema de información o que presente una amenaza de seguridad. También está prohibido:

- Descargar archivos de imágenes o videos que no tienen objetivos de negocios, enviar cadenas de correos electrónicos, jugar juegos, etc.
- Instalar software en un ordenador local sin el permiso explícito del [cago].
- Utilizar aplicaciones Java, controles Active X y otros códigos móviles, excepto cuando esté autorizado por el [cargo].
- Utilizar herramientas criptográficas (encriptado) sobre ordenadores locales, excepto en los casos especificados en la Política de Clasificación de la Información.
- Descargar códigos de programa de soportes externos.
- Instalar o utilizar dispositivos periféricos como módems, tarjetas de memoria u otros dispositivos para almacenamiento y lectura de datos (por ej., dispositivos USB) sin el permiso explícito del [cargo], el uso en conformidad con la Política de Clasificación de la Información está permitido.

### 3.5. Uso de activos fuera de las instalaciones

Los equipos, la información o software, independientemente de su formato o soporte de almacenamiento, no pueden ser retirados de las instalaciones sin el permiso escritoprevio del [cargo].

Mientras los activos en cuestión permanecen fuera de la organización, deben ser controlados por la persona a la que se le concedió el permiso para retirarlo.

### 3.6. Devolución de activos a la finalización de un contrato

Al finalizar un contrato de empleo, o de otro tipo, a raíz del cual se utilizan diversos equipos, software o información en formato electrónico o papel, el usuario debe devolver todos esos activos de información al [cargo].

### 3.7. Procedimiento para copias de seguridad

Elusuario debe especificar el método copia de seguridad toda la información sensible almacenada en su ordenador, como mínimo, una vez por día.

### 3.8. Protección antivirus

En cada ordenador debe estar instalado [nombre del antivirus] con actualización automática activada.

### 3.9. Facultados para el uso de sistemas de información

Los usuarios de los sistemas de información solamente pueden acceder a los activos de sistemas de información para los cuales han sido explícitamente autorizados por el propietario del activo.

Los usuarios pueden utilizar los sistemas de información únicamente para las actividades para las cuales han sido autorizados, es decir, para las cuales les han sido otorgados derechos de acceso.

**Comment [DK5]:** Eliminar si el control A.12.5.1 está marcado como no aplicable en la Declaración de aplicabilidad.

**Comment [DK6]:** Eliminar si no existe esta Política.

**Comment [DK7]:** Eliminar todo este punto si el controlA.11.2.5 está marcado como no aplicable en la Declaración de aplicabilidad.

**Comment [DK8]:** Se puede especificar si este permiso corresponde a una única vez o a un periodo de tiempo prolongado, o debe existir un límite de tiempo, de qué forma se concede (en papel o formato electrónico), etc.

**Comment [DK9]:** Eliminar todo este punto si el control A.8.1.4 está marcado como no aplicable en la Declaración de aplicabilidad.

**Comment [DK10]:** Eliminar todo este punto si el control A.12.3.1 está marcado como no aplicable en la Declaración de aplicabilidad.

**Comment [DK11]:** Asegúrese que esto no interfiera con la Política de procedimientos operativos para tecnología de la información y de la comunicación y Política de creación de copias de seguridad.

**Comment [DK12]:** Adaptar la frecuencia según los resultados del Análisis del impacto en el negocio, en caso que haya sido realizado.

**Comment [DK13]:** Eliminar todo este punto si el control A.12.2.1 está marcado como no aplicable en la Declaración de aplicabilidad.



©2013 Plantilla para clientes de EPPS services Ltd. www.iso27001standard.com, según Contrato de licencia.

Los usuarios no deben participar en actividades que puedan ser utilizadas para eludir controles de seguridad de los sistemas de información.

### 3.10. Responsabilidades sobre la cuenta de usuario

El usuario no debe, directa ni indirectamente, permitir que otra persona utilice sus derechos de acceso; es decir, su nombre de usuario, y no debe utilizar el nombre de usuario y/o clave de otra persona. El uso de nombres de usuario grupales está prohibido.

El propietario de la cuenta de usuario es su usuario, que es responsable de su uso y de todas las transacciones realizadas con dicha cuenta de usuario.

### 3.11. Responsabilidades sobre la clave

Los usuarios deben aplicar buenas prácticas de seguridad en cuanto a la elección y uso de claves:

- No se deben revelar las claves a otras personas, incluyendo la gerencia y los administradores del sistema.
- No se debe llevar un registro de las claves, a menos que un método seguro haya sido aprobado por [cargo].
- Las claves generadas por el usuario no deben ser distribuidas por ningún medio (oral, escrito, electrónico, etc.).
- Las claves deben ser cambiadas si existen indicios de que pueden estar en riesgo las mismas claves o el sistema (en ese caso, se debe informar un incidente de seguridad).
- Se deben escoger claves seguras de la siguiente forma:
  - utilizando al menos doce caracteres;
  - utilizando al menos un carácter numérico;
  - utilizando al menos un carácter alfabético en mayúscula y uno en minúscula;
  - utilizando al menos un carácter especial;
  - una clave no debe ser una palabra que se encuentre en el diccionario, en un dialecto o jerga de ningún idioma, como tampoco ninguna de estas palabras escritas hacia atrás;
  - las claves no deben estar relacionadas con datos personales (por ej., fecha de nacimiento, domicilio, nombre de un familiar, etc.);
  - no se deben usar nuevamente las últimas tres claves.
- Se deben cambiar las claves cada 3 meses.
- Se deben cambiar las claves en el primer ingreso al sistema.
- Las claves no deben ser almacenadas en un sistema de registro automatizado (por ej., macros o explorador).
- No se deben utilizar las mismas claves personales para fines privados y para fines comerciales.

### 3.12. Política de pantalla y escritorio limpio

Toda la información clasificada como "Uso interno", "Restringido" y "Confidencial" de acuerdo a lo establecido en la Política de Clasificación de la Información, es considerada sensible para este punto.

#### *3.12.1. Política de escritorio limpio*

**Comment [DK14]:** Eliminar si el control A.9.3.1 está marcado como no aplicable en la Declaración de aplicabilidad.

**Comment [DK15]:** Eliminar todo este punto si la Política de claves forma parte de un documento aparte.

**Comment [DK16]:** Eliminar todo este punto si el control A.9.3.1 está marcado como no aplicable en la Declaración de aplicabilidad.

**Comment [DK17]:** Eliminar todo este punto si la Política de pantalla y escritorio limpios forma parte de un documento aparte.

**Comment [DK18]:** Eliminar todo este punto si el control A.11.2.9 está marcado como no aplicable en la Declaración de aplicabilidad.



©2013 Plantilla para clientes de EPPS services Ltd. www.iso27001standard.com, según Contrato de licencia.

Si la persona autorizada no se encuentra en su puesto de trabajo, todos los documentos impresos, como también los soportes de almacenamiento de datos, etiquetados como sensibles, deben ser retirados del escritorio o de otros lugares (impresoras, equipos de fax, fotocopiadoras, etc.) para evitar el acceso no autorizado a los mismos.

Este tipo de documentos y soportes deben ser archivados de forma segura, de acuerdo a lo establecido en la Política de Clasificación de la Información.

### *3.12.2. Política de pantalla limpia*

Comment [DK19]: Eliminar todo este punto si el control A.11.2.9 está marcado como no aplicable en la Declaración de aplicabilidad.

Si la persona autorizada no se encuentra en su puesto de trabajo, se debe quitar toda la información sensible de la pantalla, y se debe denegar el acceso a todos los sistemas para los cuales la persona tiene autorización.

En el caso de una ausencia corta (hasta 30 minutos), la política de pantalla limpia se implementa finalizando la sesión en todos los sistemas o bloqueando la pantalla con una clave. Si la persona se ausenta por un período más prolongado (superior a 30 minutos), la política de pantalla limpia se implementa finalizando la sesión en todos los sistemas y apagando el puesto de trabajo.

Comment [D20]: Adaptar al sistema que se utiliza en la organización.

### *3.12.3. Protección de instalaciones y equipos compartidos*

Comment [DK21]: Eliminar este punto si el control A.11.2.8 está marcado como no aplicable en la Declaración de aplicabilidad.

Los documentos que contienen información sensible deben ser retirados inmediatamente de las impresoras, equipos de fax y fotocopiadoras.

Las instalaciones para envío y recepción de correo [indicar las instalaciones y su ubicación] están protegidas por [indicar la forma de protección cuando la persona autorizada está ausente; por ej., cerrando la instalación, etc.].

Los equipos de fax compartidos [indicar los equipos y su ubicación] están protegidos por [indicar la forma de protección cuando la persona autorizada está ausente; por ej., cerrando la instalación, etc.].

El uso no autorizado de impresoras, fotocopiadoras, escáneres y demás equipamiento compartido para copiado [indicar los equipos y su ubicación] se evita [indicar cómo; por ej., cerrando la instalación, uso de números de identificación personal, tarjetas de acceso, etc.].

## 3.13. Uso de Internet

Sólo se puede acceder a Internet a través de la red local de la organización, con la infraestructura y protección de cortafuegos adecuadas. El acceso directo a Internet mediante módems, Internet móvil, red inalámbrica u otros dispositivos de acceso directo a Internet, está prohibido.

El [cargo] puede bloquear el acceso a determinadas páginas de Internet para usuarios individuales, grupos de usuarios o para todos los empleados de la organización. Si el acceso a algunas páginas Web está bloqueado, el usuario puede elevar una petición escrita al [cargo] solicitando autorización para acceder a dichas páginas. El usuario no debe intentar eludir por su cuenta esa restricción.



©2013 Plantilla para clientes de EPPS services Ltd. www.iso27001standard.com, según Contrato de licencia.

El usuario debe considerar como no confiable la información recibida a través de sitios web no verificados. Ese tipo de información puede ser utilizado con fines comerciales solamente después de haber verificado su autenticidad y veracidad.

El usuario es responsable por todas las posibles consecuencias que surjan por el uso no autorizado o inadecuado de servicios o contenidos de Internet.

## 3.14. Correo electrónico y otros métodos de intercambio de mensajes

Entre los métodos de intercambio de mensajes, aparte del correo electrónico, se puede incluir la descarga de archivos desde Internet, la transferencia de datos por medio de [indicar los nombres de los sistemas de comunicación especializados], teléfonos, equipos de fax, el envío de mensajes de texto por teléfonos móviles, soportes móviles y foros o redes sociales.

De acuerdo con [Procedimientos operativos para tecnología de la información y de la comunicación / Política de Transferencia de la Información], como también con la [Política de Clasificación de Información], el [cargo] determina el canal de comunicación que se puede utilizar para cada tipo de dato, como también las posibles restricciones sobre quién tiene permiso para utilizar los canales, es decir, define qué actividades están prohibidas.

Los usuarios solamente pueden enviar mensajes que contengan información veraz. Está prohibido enviar materiales perturbadores, desagradables, sexualmente explícitos, groseros, difamatorios o cualquier otro contenido inaceptable o ilegal. Los usuarios no deben enviar mensajes basura a personas con las cuales no se ha establecido relación de negocios o a personas que no solicitaron ese tipo de información.

Si un usuario recibe un correo electrónico basura, debe informarlo al [cargo].

Si se envía un mensaje con una etiqueta de confidencialidad, el usuario debe protegerlo de acuerdo con lo establecido en la Política de Clasificación de Información.

El usuario debe guardar todos los mensajes que contienen datos importantes para los negocios de la organización utilizando el método especificado por el [cargo].

Cada correo electrónico debe incluir una exención de responsabilidad, salvo los mensajes enviados a través de los sistemas de comunicación determinados por el [cargo]. Si un usuario envía un mensaje a través de un sistema de intercambio de mensajes (redes sociales, foros, etc.), debe declarar sin ambigüedades que no representa el punto de vista de la organización.

## 3.15. Derechos de autor

Los usuarios no deben realizar copias no autorizadas del software que pertenece a la organización, excepto en los casos permitidos por ley, por el propietario o por el [cargo].

Los usuarios no deben copiar software ni otros materiales originales de otras fuentes, y son responsables por todas las consecuencias que pudieran surgir bajo la ley de propiedad intelectual.

## 3.16. Computación móvil

### *3.16.1. Introducción*

**Comment [DK22]:** Eliminar todo este punto si el control A.13.2.3 está marcado como no aplicable en la Declaración de aplicabilidad.

**Comment [DK23]:** Se puede especificar el soporte en cuestión.

**Comment [DK24]:** Se pueden especificar los foros y redes sociales en cuestión.

**Comment [DK25]:** Eliminar si no existe esta Política.

**Comment [DK26]:** Eliminar todo este punto si el control A.18.1.2 está marcado como no aplicable en la Declaración de aplicabilidad.

**Comment [DK27]:** Eliminar todo este punto si la Política sobre dispositivos móviles y teletrabajo forma parte de un documento aparte.

**Comment [DK28]:** Eliminar todo este punto si el control A.6.2.1 está marcado como no aplicable en la Declaración de aplicabilidad.



©2013 Plantilla para clientes de EPPS services Ltd. www.iso27001standard.com, según Contrato de licencia.

Entre los equipos de computación móvil se incluyen todo tipo de ordenadores portátiles, teléfonos móviles, tarjetas de memoria y demás equipamiento móvil utilizado para almacenamiento, procesamiento y transferencia de datos.

### *3.16.2. Reglas básicas*

Se debe tener especial cuidado cuando los equipos de computación móvil se encuentran en vehículos u otros medios de transporte, espacios públicos, habitaciones de hotel, salas de reunión, centros de conferencias y demás áreas no protegidas exteriores a las instalaciones de la organización.

La persona que se lleva equipos de computación móvil fuera de las instalaciones debe cumplir las siguientes reglas:

- El equipamiento de computación móvil que contiene información importante, sensible o crítica no debe ser desatendido y, en lo posible, debe quedar resguardado bajo llave o se deben utilizar trabas especiales para asegurarlo.
- Cuando se utiliza equipamiento de computación móvil en lugares públicos, el usuario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
- Las actualizaciones de parches y demás configuraciones del sistema son realizadas [indicar cómo se implementa técnicamente o hacer referencia a un documento que defina el proceso].
- La protección contra códigos maliciosos se instala y actualiza [indicar cómo se implementa técnicamente o hacer referencia a un documento que defina este proceso].
- La persona que utiliza equipamiento de computación móvil fuera de las instalaciones es responsable de realizar periódicamente copias de seguridad de datos [indicar cómo se implementa técnicamente o hacer referencia a un documento que defina el proceso].
- La conexión a redes de comunicación y el intercambio de datos debe reflejar la sensibilidad de los datos y se realiza [indicar cómo se implementa técnicamente o hacer referencia a un documento que defina este proceso].
- La información que se encuentra en ordenadores portátiles debe estar encriptada [indicar si es obligatorio para todo el disco duro o sólo para archivos sensibles, etc.].
- La protección de datos sensibles debe ser implementada de acuerdo con la [Política de Clasificación de Información].
- En el caso que el equipamiento de computación móvil sea desatendido, se deben aplicar las reglas para equipamiento de usuario desatendido de acuerdo a la Política de pantalla y escritorio limpios.

El [cargo] es el responsable de la capacitación y concienciación de las personas que utilizan equipamiento de computación móvil fuera de las instalaciones de la organización.

## 3.17. Tele-trabajo

Tele-trabajo significa que los equipos de información y comunicación se utilizan para permitir que los empleados realicen su trabajo fuera de la organización. El tele-trabajo no incluye el uso de teléfonos móviles fuera de las instalaciones de la organización.

El tele-trabajo debe ser autorizado por [cargo] mediante [especificar el método de autorización].

El [cargo] es el responsable de preparar planes y procedimientos para garantizar lo siguiente:

**Comment [DK29]:** Eliminar si el control A.11.2.6 está marcado como no aplicable en la Declaración de aplicabilidad.

**Comment [DK30]:** Eliminar todo este punto si la Política sobre dispositivos móviles y tele-trabajo forma parte de un documento aparte.

**Comment [DK31]:** Eliminar todo este punto si el control A.6.2.2 está marcado como no aplicable en la Declaración de aplicabilidad.

**Comment [D32]:** La autorización puede ser concedida de forma oral o escrita, por medio de un correo electrónico o firmando un documento, puede ser más o menos formal, etc.

**Comment [D33]:** En las empresas más pequeñas no es necesario documentarlo, identificando las reglas establecidas debería ser suficiente.



©2013 Plantilla para clientes de EPPS services Ltd. www.iso27001standard.com, según Contrato de licencia.

- Protección del equipamiento de computación móvil, de acuerdo a lo indicado en la sección anterior.
- Evitar el acceso no autorizado de personas que viven o trabajan en la ubicación donde se realiza la actividad de tele-trabajo.
- Configuración adecuada de la red local utilizada para conectarse a la Internet.
- Protección de los derechos de propiedad intelectual de la organización, tanto por el software como por otros contenidos que puedan estar protegidos por derechos de propiedad intelectual.
- Proceso de devolución de datos y equipamiento en caso de finalización del empleo.
- Nivel mínimo de configuración de la instalación donde se realizarán las actividades de tele-trabajo.
- Tipos de actividades permitidas y prohibidas.

### 3.18. Supervisión del uso de sistemas de información y comunicación

Todos los datos creados, almacenados, enviados o recibidos a través del sistema de información, o de otro sistema de comunicación, de la organización, incluyendo diversas aplicaciones, correo electrónico, Internet, fax, etc., independientemente de si es personal o no, se considera propiedad de [nombre de la organización].

Los usuarios aceptan que personas autorizadas de la organización puedan acceder a todos los datos de ese tipo y que el acceso de dichas personas no será considerado una violación de privacidad del usuario.

La organización puede utilizar herramientas especializadas para identificar y bloquear métodos prohibidos de comunicación y para filtrar contenidos prohibidos.

### 3.19. Incidentes

Cada empleado, proveedor o tercero que esté en contacto con datos y/o sistemas de [nombre de la organización] debe reportar toda debilidad del sistema, incidente o evento que pudiera derivar en un posible incidente, de acuerdo a lo establecido en el Procedimiento para gestión de incidentes.

## 4. Gestión de registros guardados en base a este documento

| Nombre del registro | Ubicación de archivo | Persona responsable del archivo | Controles para la protección del registro | Tiempo de retención |
|---|---|---|---|---|
| [Autorizaciones para instalación de software, uso de aplicaciones Java y controles Active X, uso de herramientas criptográficas, descarga de | [carpeta de Intranet] | [cargo] | Los registros no pueden ser editados, sólo el [cargo] puede guardar estos registros | Los registros son almacenados por el plazo de 3 años |

**Comment [D34]:** Modificar según sea necesario.



©2013 Plantilla para clientes de EPPS services Ltd. www.iso27001standard.com, según Contrato de licencia.

| | | | | |
|---|---|---|---|---|
| códigos de programas desde soportes externos, instalación de dispositivos periféricos] - formato electrónico | | | | |
| [Autorizaciones para retirar activos fuera de las instalaciones] - formato electrónico | [carpeta de Intranet] | [cargo] | Los registros no pueden ser editados, sólo el [cargo] puede guardar estos registros | Los registros son almacenados por el plazo de 3 años |
| [Autorización para acceder a determinadas páginas de Internet] - formato electrónico | [carpeta de Intranet] | [cargo] | Los registros no pueden ser editados, sólo el [cargo] puede guardar estos registros | Los registros son almacenados por el plazo de 3 años |
| [Decisión acerca de cómo se puede intercambiar cada tipo de datos] - formato electrónico | [carpeta de Intranet] | [cargo] | Los registros no pueden ser editados, sólo el [cargo] puede guardar estos registros | Los registros son almacenados por el plazo de 3 años |
| [Decisión acerca de cómo se deben almacenar los mensajes que contienen datos importantes para el negocio] - formato electrónico | [carpeta de Intranet] | [cargo] | Los registros no pueden ser editados, sólo el [cargo] puede guardar estos registros | Los registros son almacenados por el plazo de 3 años |
| [Autorización para tele-trabajo] - formato electrónico | [carpeta de Intranet] | [cargo] | Los registros no pueden ser editados, sólo el [cargo] puede guardar estos registros | Los registros son almacenados por el plazo de 3 años |

**Comment [D35]:** Modificar según sea necesario.

**Comment [D36]:** Modificar según sea necesario.

**Comment [D37]:** Modificar según sea necesario.

**Comment [D38]:** Modificar según sea necesario.

**Comment [D39]:** Modificar según sea necesario.

Solamente el [cargo] puede permitir a otros empleados el acceso a cualquiera de los documentos mencionados precedentemente.



©2013 Plantilla para clientes de EPPS services Ltd. www.iso27001standard.com, según Contrato de licencia.

## 5. Validez y gestión de documentos

Este documento es válido desde el [fecha]

El propietario de este documento es el [cargo], que [illegible] documento por lo menos una vez al año.

**Comment [DK40]:** Esto es sólo una recomendación; ajustar la frecuencia según sea necesario.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de incidentes [illegible] de información.
- Cantidad de incidentes relacionados con [illegible] o de [illegible].

[cargo]
[nombre]

_____
[firma]

**Comment [DK41]:** Sólo es necesario si el Procedimiento para control de documentos y registros establece que los documentos en papel deben ser firmados.



©2013 Plantilla para clientes de EPPS services Ltd. www.iso27001standard.com, según Contrato de licencia.