[logo de la organización]

[nombre de la organización]

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

PROCEDIMIENTOS OPERATIVOS PARA TECNOLOGÍA DE LA INFORMACIÓN Y DE LA COMUNICACIÓN

Comment [DK2]: Las partes de este documento para las que se necesita realizar una especificación más detallada, pueden ser redactas como documentos separados (políticas/procedimientos).

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

Comment [DK3]: 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. PROCEDIMIENTOS OPERATIVOS PARA TECNOLOGÍA DE LA INFORMACIÓN Y DE LA COMUNICACIÓN 3

3.1. GESTIÓN DE CAMBIO 3
3.2. COPIAS DE SEGURIDAD 4
3.2.1. Procedimiento para copias de seguridad 4
3.2.2. Prueba de las copias de seguridad 4
3.3. GESTIÓN DE SEGURIDAD DE RED 4
3.4. SERVICIOS DE RED 5
3.5. ELIMINACIÓN Y DESTRUCCIÓN DE EQUIPOS Y SOPORTES 5
3.5.1. Equipos 5
3.5.2. Soportes móviles de almacenaje 5
3.5.3. Soportes en papel 5
3.5.4. Borrado y destrucción de registros; comisión para la destrucción de datos 5
3.6. TRANSFERENCIA DE LA INFORMACIÓN 6
3.6.1. Canales de comunicación electrónica 6
3.6.2. Relaciones con entidades externas 6
3.7. SUPERVISIÓN DEL SISTEMA 6

4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO 7

5. VALIDEZ Y GESTIÓN DE DOCUMENTOS 8

©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 garantizar el funcionamiento correcto y seguro de la tecnología de la información y de la comunicación.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a toda la tecnología de la información y de la comunicación, como también a la documentación relacionada dentro del alcance del SGSI.

Los usuarios de este documento son empleados de [unidad organizativa de tecnología de la información y de la comunicación].

2. Documentos de referencia

- Norma ISO/IEC 27001, capítulos A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.14.2.4
- Política de Seguridad de la Información
- [Estrategia de continuidad del negocio]
- [Política sobre el uso de los servicios en red]
- [Política sobre dispositivos móviles y tele-trabajo]
- [Política de Clasificación de la Información]
- [Inventario de activos]
- [Política de seguridad para proveedores]

3. Procedimientos operativos para tecnología de la información y de la comunicación

3.1. Gestión de cambio

Cualquier cambio sobre sistemas operativos o de producción debe ser realizado de la siguiente forma:

1. Los cambios [indicar los cargos].
2. Los cambios deben ser autorizados por el [cargo], que debe para el .
3. Los cambios deben ser implementados por [cargo].
4. El [cargo] es el de acuerdo al requerimiento.
5. El [cargo] es el responsable de probar y verificar la : el sistema no .
6. La implementación de personas: [detallar todos los cargos necesarios]

[indicar el nombre del formulario o informar un método diferente para registrar los cambios].

Comment [DK4]: Eliminar todo este punto si el control A.12.1.2 está marcado como no aplicable en la Declaración de aplicabilidad.

Comment [DK5]: Eliminar este punto si la Política de gestión de cambio forma parte de un documento aparte.

Comment [DK6]: Se puede especificar cambios de configuración, etc.

Comment [DK7]: Otra forma de quién será la persona responsable para cada paso.

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

3.2. Copias de seguridad

3.2.1. Procedimiento para copias de seguridad

Se deben crear copias de seguridad para todos los sistemas identificados en la [Estrategia de continuidad del negocio] y con la frecuencia especificada en dicho documento.

El [cargo] es el responsable de crear copias de seguridad de información, software e imágenes del sistema. [Si fuera necesario, detallar qué tecnología se utiliza para crear las copias de seguridad, indicar las responsabilidades sobre las actividades individuales, las ubicaciones para almacenar las copias, la protección física que tienen, encriptado, claves, etc.]

Se crean automáticamente registros del proceso de creación de copias de seguridad en los sistemas sobre los que se realiza la copia de seguridad.

3.2.2. Prueba de las copias de seguridad

Las copias de seguridad y el proceso de restauración deben ser probados al menos [una vez cada tres meses] mediante la implementación del proceso de recuperación de datos en [identificar el servidor en el cual se realiza la recuperación de datos] y la verificación de que todos los datos han sido recuperados satisfactoriamente.

El [cargo] es el responsable de probar las copias de seguridad. Los registros de las pruebas realizadas sobre las copias de seguridad se llevan [indicar el formato del registro (en papel o electrónico), si hay un formulario determinado, etc.].

3.3. Gestión de seguridad de red

El [cargo] es el responsable de gestionar y controlar las redes de computación, de garantizar la seguridad de la información en las redes y de proteger los servicios conectados a la red desde accesos no autorizados. Por lo tanto, es necesario:

- Separar la responsabilidad operativa de las redes de la responsabilidad sobre aplicaciones sensible y demás sistemas.
- Proteger los datos sensibles que se transmiten por la red pública [describir la tecnología que se utiliza para la protección y especificar las responsabilidades y las personas responsables].
- Proteger los datos sensibles que se transmiten por redes inalámbricas [describir la tecnología que se utiliza para la protección y especificar las responsabilidades y las personas responsables].
- Proteger a los equipos que se conectan a la red desde ubicaciones remotas [describir la tecnología que se utiliza para la protección y especificar las responsabilidades y las personas responsables].
- Separar el tráfico que ingresa por dispositivos móviles, establecer políticas exclusivas de cortafuegos, rutas estáticas, redes virtuales de área local, etc.
- Garantizar la disponibilidad de los servicios en red [describir los controles que asegurarán la disponibilidad].
- El [cargo] debe periódicamente verificar y probar los controles implementados.

Comment [DK8]: Eliminar todo este punto si el control A.12.3.1 está marcado como no aplicable en la Declaración de aplicabilidad.

Comment [DK9]: Eliminar este punto si la Política para creación de copias de seguridad forma parte de un documento aparte.

Comment [DK10]: En caso que no exista este documento, se deben enumerar aquí todos los sistemas o los que se les tiene que realizar copias de seguridad, indicando también con qué frecuencia.

Comment [DK11]: Las copias de seguridad deben ser almacenadas en ubicaciones suficientemente alejadas de la ubicación principal para que no sean afectadas por un desastre.

Comment [DK12]: Adaptar la frecuencia de acuerdo con el riesgo evaluado.

Comment [DK13]: Eliminar todo este punto si el control A.13.1.1 está marcado como no aplicable en la Declaración de aplicabilidad.

Comment [DK14]: O hacer referencia a la Política sobre dispositivos móviles y teletrabajo.

Comment [DK15]: Se puede especificar la frecuencia; por ej., diariamente o en algunos días del mes, etc.

Comment [DK16]: Se pueden especificar los controles por ej. cortafuegos, sistemas de detección de intrusiones, etc.

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

3.4. Servicios de red

El [cargo] debe definir las características de seguridad y el nivel de servicio deseado para todos los servicios en red, si estos servicios son prestados por la empresa o son tercerizados. Se deberán documentar estos servicios con los proveedores.

Si los servicios de red son externalizados, se deben especificar los requerimientos en el acuerdo según se define en la [Política de seguridad para proveedores].

3.5. Eliminación y destrucción de equipos y soportes

Todos los datos y software con licencia almacenados en soportes móviles (por ej., CD, DVD, unidades USB, tarjetas de memoria, etc., y también en papel) y en todos los equipos que tienen soportes de almacenaje (por ej., ordenadores, teléfonos móviles, etc.) deben ser borrados, o se debe destruir el soporte, antes de ser eliminados o reutilizados.

La persona responsable de borrar los datos o destruir el soporte debe informar al propietario del activo en cuestión acerca del borrado o eliminación de datos, y el propietario del activo debe actualizar el Inventario de activos.

3.5.1. Equipos

El [cargo] es el responsable de verificar y borrar datos de los equipos, salvo que la Política de clasificación de la información establezca otra cosa. Los datos deben ser borrados [indicar la tecnología utilizada para el borrado de datos en los soportes de los equipos], pero si, teniendo en cuenta la sensibilidad de los datos, el proceso no es suficientemente seguro, entonces los soportes de almacenaje deben ser destruidos.

3.5.2. Soportes móviles de almacenaje

El [cargo] es el responsable de borrar datos de los soportes móviles de almacenaje, salvo que la Política de clasificación de la información establezca otra cosa. Los datos deben ser borrados [indicar la tecnología utilizada para el borrado de datos en los soportes], pero si, teniendo en cuenta la sensibilidad de los datos, el proceso de borrado no es suficientemente seguro, entonces los soportes de almacenaje deben ser destruidos.

3.5.3. Soportes en papel

Los empleados de la organización que manejan documentos individuales son responsables de destruir los soportes en papel, salvo que la Política de clasificación de la información establezca otra cosa. Los documentos en papel se destruyen en trituradoras de papel.

3.5.4. Borrado y destrucción de registros; comisión para la destrucción de datos

Se deben llevar registros de todo el borrado o destrucción de datos clasificados como "Restringido" y "Confidencial". Los registros deben incluir la siguiente información: datos sobre los soportes, fecha de borrado o destrucción, método de borrado o destrucción, persona que realizó el proceso.

Comment [DK17]: Eliminar todo este punto si los controles A.8.3.2 y A.11.2.7 están marcados como no aplicables en la Declaración de aplicabilidad.

Comment [DK18]: Eliminar este punto si la Política de eliminación y destrucción forma parte de un documento aparte.

Comment [DK19]: Es posible aclarar que este significa almacenamiento en la propia organización y/o transferencia a otra organización (por ej., por una venta, donación, envío a servicio de reparación, etc.).

Comment [DK20]: Es posible aclarar que esto significa que es entregado a otro usuario, etc.

Comment [DK21]: Eliminar este punto si el control A.8.1.1 está marcado como no aplicable en la Declaración de aplicabilidad.

Comment [DK22]: Eliminar si no existe esta Política.

Comment [DK23]: Por ej., enumerar herramientas especializadas que se deben utilizar, especificar si se utiliza, y de qué forma, el proceso de sobre escritura de datos con ceros.

Comment [DK24]: Esto puede ser, por ejemplo, un disco duro de un servidor.

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

Comment [DK26]: Eliminar si no existe esta Política.

Comment [DK27]: Si especificar alguna otra tecnología.

Comment [DK28]: Adaptar a los niveles de confidencialidad que se utilizan en la organización.

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

Toda la información clasificada como "Confidencial" debe ser borrada o destruida ante la presencia de una comisión integrada por personas autorizadas a acceder a dicha información.

3.6. Transferencia de la información

3.6.1. Canales de comunicación electrónica

La información de la organización puede ser intercambiada a través de los siguientes canales de comunicación electrónica: correo electrónico, descarga de archivos desde Internet, transferencia de datos por medio de [indicar los nombres de los sistemas de comunicación especializados], teléfonos, equipos de fax, mensajes de texto por teléfonos móviles, soportes móviles, foros o redes sociales.

El [cargo] determina qué canales de comunicación se pueden utilizar para cada tipo de información y las posibles restricciones sobre los permisos para usar dichos canales, es decir, define qué actividades están prohibidas.

Además de los controles establecidos por la Política de clasificación de la información , el [cargo] determina controles adicionales para cada tipo de datos y canales de comunicación según los resultados de la evaluación de riesgos.

3.6.2. Relaciones con entidades externas

Entre las entidades externas se incluyen a diversos proveedores de servicios, empresas de mantenimiento de software y hardware, empresas que manejan transacciones o procesamiento de datos, clientes, etc.

Antes de intercambiar información y/o software con cualquier entidad externa, se debe firmar un contrato, el cual es responsabilidad del [cargo]. El contrato puede estar en papel o en formato electrónico (por ejemplo, aceptando los términos y condiciones generales) y debe contener cláusulas que coincidan con la evaluación de riesgos, incluyendo, al menos, las siguientes:

- Método de identificación de la otra parte.
- Autorizaciones para acceder a la información.
- Asegurar la inviolabilidad.
- Estándares técnicos para la transferencia de datos.
- Respuesta a incidentes.
- Etiquetado y manejo de información sensible.
- Derechos de autor.

Los acuerdos con terceros externos deben ser confeccionados de acuerdo con la [Política de seguridad para proveedores].

3.7. Supervisión del sistema

En base a los resultados de la evaluación de riesgos, el [cargo] decide qué registros se guardarán en qué sistemas, para qué sistemas y por cuánto tiempo. Se deben guardar los registros para todos los administradores y operadores de sistema sobre sistemas sensibles.

Comment [DK29]: Eliminar este punto si la Política de transferencia de información forma parte de un documento aparte.

Comment [DK30]: Eliminar todo este punto si el control A.13.2.1 está marcado como no aplicable en la Declaración de aplicabilidad.

Comment [DK31]: Se puede especificar el soporte en cuestión.

Comment [DK32]: Se pueden especificar los foros o redes sociales en cuestión.

Comment [DK33]: Agregar o eliminar canales de comunicación de acuerdo con la evaluación de riesgos o con los canales utilizados habitualmente en la organización.

Comment [DK34]: Este texto puede ser reemplazado directamente estableciendo el tipo de datos y los canales de comunicación, las restricciones y las actividades prohibidas.

Comment [DK35]: Eliminar si no existe esta Política.

Comment [DK36]: Eliminar todo este punto si el control A.13.2.2 está marcado como no aplicable en la Declaración de aplicabilidad.

Comment [DK37]: Entre los registros se pueden incluir actividades del usuario, actividades del administrador y del operador de sistema, excepciones, eventos de seguridad, etc.

Comment [DK38]: Eliminar este texto si el control A.12.4.1 está marcado como no aplicable en la Declaración de aplicabilidad.

Comment [DK39]: Eliminar este texto si el control A.12.4.3 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.

El [cargo] es el responsable de supervisar diariamente los registros de los fallos informados en forma automática, como también de registrar los fallos informados por los usuarios, de analizar por qué se produjeron los errores y de aplicar las acciones correctivas correspondientes. [Se pueden indicar autorizaciones específicas para acciones en caso de error, como también cómo se guardan los registros sobre los errores]

El [cargo] es el responsable de revisar periódicamente los registros para verificar las actividades de los usuarios, administradores y operadores de sistemas. La supervisión se realiza de acuerdo a intervalos determinados por el [cargo], que es quien establece y escoge los registros para supervisar y determina cómo se registrará la supervisión. Se debe informar al [cargo] acerca de los resultados de la revisión.

Comment [DK40]: Eliminar este texto si los controles A.12.4.1 y A.12.4.3 están marcados como no aplicables en la Declaración de aplicabilidad.

Comment [DK41]: Se puede especificar que aquí se incluye, por ejemplo, la supervisión de correo u demás comunicación electrónica, lo cual debe cumplir con la legislación local.

Comment [DK42]: Si fuera necesario, esto se puede determinar en forma mucho más detallada, por ejemplo, en un cuadro, qué sistemas se revisan, con qué frecuencia, etc.

Comment [DK43]: Eliminar este texto si los controles A.12.4.1 y A.12.4.3 están marcados como no aplicables en la Declaración de aplicabilidad.

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
[Nombre del registro de cambio] - en formato electrónico	[Nombre de carpeta de Intranet]	[cargo]	Una vez creado, el registro ya no puede ser modificado.	3 años
[Decisiones sobre los canales de comunicación utilizados para tipos específicos de información, restricciones, actividades prohibidas] - formato electrónico	[Nombre de carpeta de Intranet]	[cargo]	Una vez creado, el registro ya no puede ser modificado.	3 años
[Registros del proceso para copias de seguridad] - formato electrónico	Sistema que ejecuta el procedimiento de copias de seguridad	[cargo]	Los registros son de sólo lectura, no pueden ser eliminados ni editados	Los registros son almacenados por el plazo de 1 año
[Registros de las pruebas realizadas sobre las copias de seguridad] - en papel o formato electrónico	[nombre de la carpeta de archivo o gabinete]	[cargo]	Solamente el [cargo] tiene el derecho para acceder a estos registros	Los registros son almacenados por el plazo de 1 año

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

[Características de seguridad y nivel de servicio deseado para servicios en red] - formato electrónico o papel	Ordenador del [cargo], [nombre de la carpeta de archivo o gabinete]	[cargo]	Solamente el [cargo] tiene el derecho para acceder a estos registros	5 años luego del vencimiento del acuerdo o del servicio prestado
[Borrado o destrucción de registros] - en papel	[nombre de la carpeta de archivo o gabinete]	[cargo]	El gabinete tiene cerradura, las llaves están en custodia de [cargos]	Los registros son almacenados por el plazo de 5 años
[Evidencia de revisión de registros] - en formato electrónico y papel	Ordenador del [cargo], [nombre de la carpeta de archivo o gabinete]	[cargo]	Solamente el [cargo] tiene el derecho para acceder a estos registros	Los registros son almacenados por el plazo de 5 años

5. Validez y gestión de documentos

Este documento es válido desde el [fecha]

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

Comment [DK44]: 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 [illegible] los sistemas de TIC.
- Cantidad de [illegible] funcionamiento de los sistemas de TIC.

[cargo]
[nombre]

_____
[firma]

Comment [DK45]: 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.