Índice

1. Motivación del proyecto 3
2. Objetivos 3
3. Conceptos básicos 4
	1. Concepto
	2. ¿SGSI?
	3. ISO/IEC
	4. Métrica
	5. L.O.P.D
4. Análisis inicial 7
	1. Información básica
	2. Información técnica
	3. Distribución organización
	4. Bases de datos
	5. Cuentas correos
	6. Copias de seguridad
	7. Seguridad física
	8. Seguridad lógica
	9. Mapa de red
5. Implantación sistema gestor de seguridad de la información 10
	1. Fase 1
	2. Alcance
	3. Políticas y objetivos de la seguridad
	4. Controles implantados
	5. Conclusiones
6. Red y medidas de seguridad 25
	1. Mapa de red
	2. Documento de confidencialidad
	3. Cuentas de usuarios
	4. Autentificación
	5. Passwords
	6. Permisos a la base de datos
	7. Inactividad
7. Políticas de seguridad de la información 28
	1. Políticas de seguridad para equipos y empleados
	2. Políticas de seguridad para router
	3. Políticas de seguridad para servidor
	4. Políticas de seguridad para BBDD
	5. Políticas de seguridad para Correo electrónico
	6. Políticas de seguridad para Backups
8. Organización de la seguridad de la información 34
	1. Asignación responsabilidades
	2. Responsabilidad por los activos
	3. Clasificación de la información
	4. Seguridad de los recursos humanos
	5. Seguridad física y ambiental
	6. Control de acceso a equipos
	7. Transporte
9. Protección contra Malware 36
	1. Antivirus
	2. Malware
	3. Firewall
	4. Ataques de red
	5. Web
10. Gestión de seguridad de redes 37
11. Gestión de riesgos 37
	1. Análisis de riesgos
	2. Activos y factores de riesgos
	3. Posibles consecuencias
12. Plan de contingencias 48
	1. Administración de incidentes
	2. Backup de equipamiento
	3. Plan de recuperación
13. App de gestión 52
14. Conclusiones 52
15. Bibliografía 54
16. Anexos

# 1 Razón del proyecto

 La evolución continua de las tecnologías y la repentina aparición del Big data producen un flujo de información de carácter personal continuo el cual debe ser tratado y administrado de modo correcto.

Hoy en día cualquier empresa por pequeña que sea procesa una gran cantidad de información.

Hasta ahora no se ha dado la importancia que le pertenece a mantener estos datos sensibles a buen recaudo.

Gracias a la ISO/IEC 27001 se añade un nuevo concepto de indicador sobre la eficacia de los controles, lo cual provoca que el Sistema de Gestión de Seguridad de la Información sea capaz de evaluar su calidad y su eficacia.

Para ello implementaré un SGSI en una empresa del sector servicios siguiendo las pautas para recibir la certificación ISO 27001.

# 2 Objetivos

* Analizar en profundidad la empresa y su SGSI
* Establecer un SGSI para la protección de sus activos
* Preparar la empresa para la certificación ISO 27001
* Encontrar y analizar fisuras en la seguridad de la empresa

# 3 Introducción

***3.1 Concepto***

Es un estándar de seguridad publicado por la organización internacional para la estandarización y la comisión de electrotécnica internacional publicado como estándar internacional en octubre de 2005 por [International Organization for Standardization](https://es.wikipedia.org/wiki/International_Organization_for_Standardization) y por la comisión [International Electrotechnical Commission](https://es.wikipedia.org/wiki/International_Electrotechnical_Commission).

Contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los sistemas de gestión de la seguridad de la información (SGSI).

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada.

***3.2 ¿SGSI?***

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la

Seguridad de la Información.

Es el concepto central sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

• Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

• Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

• Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

Para implementar y gestionar un SGSI en base a la ISO 27001 se utiliza el ciclo continuo

PLANIFICAR-HACER-VERIFICAR-ACTUAR

* Planificar: Establecer el SGSI
* Hacer: implementar y utilizar el SGSI
* Verificar: monitorizar y revisar el SGSI
* Actuar: mantener y mejorar el SGSI



***3.3 ISO/IEC***

Son estándares de seguridad publicados por la Comisión Electrotécnica Internacional (IEC) y la Organización Internacional para la Estandarización (ISO). La serie ISO/IEC 27000 sirve para desarrollar, mantener e implementar especificaciones para los sistemas de gestión de la seguridad de la información, también conocido como (SGSI).

Las Normas ISO nos ayudan a aplicar las nuevas tecnologías a la vida diaria de la empresa y a gestionar adecuadamente los recursos de esta. Es por esta razón que a las empresas les resulta de especial utilidad la implantación de las normas ISO que mejor se adapten a su caso. Las normas ISO contribuyen positivamente al mundo en el que vivimos, facilitan el comercio, difunden el conocimiento, propagan los avances innovadores en tecnología y comparten buenas prácticas de gestión y de evaluación de la conformidad.

Estos factores son de vital importancia ya no tanto en grandes empresas sino en medianas empresas para volverla mucho más competitivas y conseguir un espacio en el sector de las grandes empresas donde la eficiencia y eficacia se convierten en un requisito indispensable.

***3.4 Métrica***

El uso de las métricas nos sirven para poder entender el proceso técnico que se está aplicando para crear o desarrollar un producto, ya que a través de ellas somos capaces de medir dicho producto para saber cómo mejorar su calidad.

***3.5 L.O.P.D***

Es una [Ley Orgánica](https://es.wikipedia.org/wiki/Ley_Org%C3%A1nica) [española](https://es.wikipedia.org/wiki/Espa%C3%B1a) que tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los [derechos fundamentales](https://es.wikipedia.org/wiki/Derechos_fundamentales) de las personas físicas, y especialmente de su [honor](https://es.wikipedia.org/wiki/Honor), [intimidad](https://es.wikipedia.org/wiki/Intimidad) y [privacidad](https://es.wikipedia.org/wiki/Privacidad) personal y familiar.

# 4 Estudio Inicial

En el año 2011 Kuups (empresa participada al 100% por Nudisco, S.L.) adquiere la marca Vidal Tiendas Supermercados, junto con los 16 establecimientos y el centro logístico de Montaverner (Valencia) que continuaban en activo. Actualmente dispone de 30 supermercados repartidos por la Comunidad Valenciana y Barcelona

***4.1 Información básica***

Nombre: Vidal tiendas y supermercados

Ubicación: Onteniente

No trabajadores: 700

Campos de trabajo: Sector servicios

***4.2 Información técnica***

No equipos: 700

Sistema operativo: Windows XP y Windows 8

Periféricos

• Multifunción

• Fax

Conexión Internet

• 6 MB Simétricos

•30 MB Simétricos

•3G

***4.3 Distribución organización***

La sede de la empresa se encuentra en Onteniente, en la parte alta del mismo supermercado, posee diversos centros logísticos.

En Onteniente se estable el centro de procesamiento de datos donde están instalados los servidores en racks.

Todos los supermercados y centro logísticos permanecen interconectados por VPN.

 ***4.4 Bases de datos***

Existen diversas bases de datos con amplia información:

•Datos de los empleados: Contiene ID de usuarios, departamento del empleado, permisos y restricciones…

• Datos de asesoramiento laboral: Contratos, nóminas, finiquitos, certificaciones de cotización, altas/bajas, altas y bajas en mutua de accidentes, cotizaciones y partes de incapacidad temporal a la seguridad social. Estos datos son realizados mensualmente en papel y mediante ficheros digitales generados por programas específicos.

• Datos contables: La organización dispone en formato de papel los documentos contables como facturas, extractos bancarios. etc. También dispone de estos datos en formato digital creados con programas específicos para este fin.

•Datos de todos los productos y ventas.

 ***4.5 Cuentas correos***

La empresa dispone de un dominio y servidor de correo.

 ***4.6 Copias de seguridad***

Se realizan distintas copias de seguridad tanto diarias, como semanales y diarias que son almacenadas en los servidores de backup en RAID.

 ***4.7 Seguridad física***

El CPD dispone de una puerta blindada protegida con pin y llave, también dispone de extracción de humos y extinción de fuegos mediante CO2.

 ***4.8 Seguridad lógica***

La empresa dispone de una versión corporativa de Panda Antivirus, de manera que en el servidor existe una versión instalada para este y en el resto de los equipos una versión de AVG antivirus.

 ***4.9 Mapa de red***



# 5 Implantación sistema gestor de seguridad de la información

***5.1 Fase 1***

Analizar la situación actual y evaluar la seguridad objetivo: Identificar los objetivos de negocio, ya que el propósito de la certificación es garantizar la gestión de la seguridad sin perder de vista que esta ayude al desarrollo de las actividades comerciales de la organización.

***5.2 Alcance***

En el SGSI se incluirá:

• Todos los datos de carácter personal que esta tiene a su disposición tanto en formato digital como impreso.

• Activos materiales de la que esta dispone, PC, portátiles, lápices USB, copias de seguridad...

• También se incluye en el SGSI la red de la organización.

• Las cuentas de correo

• Transacciones electrónicas y telemáticas.

• Seguridad física del local donde se trabaja

***5.3 Políticas y objetivos de la seguridad***

La dirección y gerencia de Vidal Tiendas y Supermercados se compromete y acepta cumplir todo lo referente al Sistema de Gestión de Seguridad de la información y formar a todos sus empleados para una correcta implantación y cumplimiento de la ISO 27001 que ayudara a mantener la integridad, confidencialidad y disponibilidad de los datos de la organización, así como el cumplimiento de la ley de protección de datos.

***5.4 Controles implantados***

Se comprueba que controles de la norma están implantaos y a qué nivel en base a un checklist, para determinar el grado de madurez en el que se encuentra la compañía, para poder identificar el esfuerzo que hay que hacer en la implementación.

## **Tabla A.1 Objetivos de control y controles**

|  |
| --- |
| **A.5 Política de seguridad** |
| ***A.5.1 Política de seguridad de la información****Objetivo*: Proporcionar indicaciones para la gestión y soporte de la seguridad de la información de acuerdo con los requisitos empresariales y con la legislación y las normativas aplicables. |
| **No implementado** | Documento de política de seguridad de la información | *Control* La Dirección debe aprobar un documento de po- lítica de seguridad de la información, publicarlo y distri- buirlo a todos los empleados y terceros afectados. |
| **No implementado** | Revisión de la política de seguridad e la información | *Control* La política de seguridad de la información debe revisarse a intervalos planificados o siempre que se pro- duzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia. |
| **A.6 Aspectos organizativos de la seguridad de la información** |
| ***A.6.1 Organización interna****Objetivo:* Gestionar la seguridad de la información dentro de la organización. |
| **No implementado** | Comité de gestión de seguridad de la información. | *Control* La Dirección debe prestar un apoyo activo a la seguridad dentro de la organización a través de directrices claras, un compromiso demostrado, asignaciones explícitas y el reconocimiento de las responsabilidades de seguridad de la información. |
| **No implementado** | Coordinación de la seguridad de la información | *Control* Las actividades relativas a la seguridad de la in- formación deben ser coordinadas entre los representantes de las diferentes partes de la organización con sus corres- pondientes roles y funciones de trabajo. |
| **Implementado** | Asignación de responsabilidades relativas a la seguridad de la información | *Control* Deben definirse claramente todas las responsabi- lidades relativas a la seguridad de la información. |
| **No implementado** | Proceso de autorización de recursos para el procesado de la información | *Control* Para cada nuevo recurso de procesado de la in- formación, debe definirse e implantarse un proceso de autorización por parte de la Dirección. |
| **No implementado** | Acuerdos de confidencialidad | *Control* Debe determinarse y revisarse periódicamente la necesidad de establecer acuerdos de confidencialidad o no revelación, que reflejen las necesidades de la organización para la protección de la información. |

|  |  |  |
| --- | --- | --- |
| A.6.1.6 | Contacto con las autoridades | *Control* Deben mantenerse los contactos adecuados con las autoridades competentes. |
| A.6.1.7 | Contacto con grupos de especial interés | *Control* Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros, y asociaciones profesionales especializadas en seguridad. |
| A.6.1.8 | Revisión independiente de la seguridad de la información | *Control* El enfoque de la organización para la gestión de la seguridad de la información y su implantación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para la seguridad de la información), debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad. |
| ***A.6.2 Terceros****Objetivo:* Mantener la seguridad de la información de la organización y de los dispositivos de procesado de la información que son objeto de acceso, tratamiento, comunicación o gestión por terceros. |
| **No implementado** | Identificación de los riesgos derivados del acceso de terceros | *Control* Deben identificarse los riesgos para la informa- ción y para los dispositivos de procesado de la información de la organización derivados de los procesos de negocio que requieran de terceros, e implantar los controles apropiados antes de otorgar el acceso. |
| **Implementado** | Tratamiento de la seguridad en la relación con los clientes | *Control* Antes de otorgar acceso a los clientes a los activos o a la información de la organización, deben tratarse todos los requisitos de seguridad identificados. |
| **Implementado** | Tratamiento de la seguridad en contratos con terceros | *Control* Los acuerdos con terceros que conlleven acceso, tratamiento, comunicación o gestión, bien de la información de la organización, o de los recursos de tratamiento de la información, o bien la incorporación de productos o servicios a los recursos de tratamiento de la información, deben cubrir todos los requisitos de seguridad pertinentes. |
| **A.7 Gestión de activos** |
| ***A.7.1 Responsabilidad sobre los activos****Objetivo:* Conseguir y mantener una protección adecuada de los activos de la organización. |
| **Implementado** | Inventario de activos | *Control* Todos los activos deben estar claramente identifi- cados y debe elaborarse y mantenerse un inventario de todos los activos importantes. |
| **Implementado** | Propiedad de los activos | *Control* Toda la información y activos asociados con los recursos para el tratamiento de la información deben tener un propietario3) que forme parte de la organización y haya sido designado como propietario |
| **No implementado** | Uso aceptable de los activos | *Control* Se deben identificar, documentar e implantar las reglas para el uso aceptable de la información y los activos asociados con los recursos para el procesado de la información. |

|  |
| --- |
| ***A.7.2 Clasificación de la información****Objetivo:* Asegurar que la información recibe un nivel adecuado de protección. |
| **No implementado** | Directrices de clasificación | *Control* La información debe ser clasificada según su valor, los requisitos legales, la sensibilidad y la criticidad para la organización. |
| **No implementado** | Etiquetado y manipulado de la información | *Control* Se debe desarrollar e implantar un conjunto adecuado de procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación adoptado por la organización. |
| **A.8 Seguridad ligada a los recursos humanos** |
| ***A.8.1 Antes del empleo***4)*Objetivo:* Asegurar que los empleados, los contratistas y los terceros entienden sus responsabilidades, y son adecuados para llevar a cabo las funciones que les corresponden, así como para reducir el riesgo de robo, fraude o de uso indebido de los recursos. |
| **No implementado** | Funciones y responsabilidades | *Control* Las funciones y responsabilidades de seguridad de los empleados, contratistas y terceros se deben definir y documentar de acuerdo con la política de seguridad de la información de la organización. |
| **Implementado** | Investigación de antecedentes | *Control* La comprobación de los antecedentes de todos los candidatos al puesto de trabajo, de los contratistas o de los terceros, se debe llevar a cabo de acuerdo con las legisla- ciones, normativas y códigos éticos que sean de aplicación y de una manera proporcionada a los requisitos del negocio, la clasificación de la información a la que se accede y los riesgos considerados. |
| **Implementado** | Términos y condiciones de contratación | *Control* Como parte de sus obligaciones contractuales, los empleados, los contratistas y los terceros deben aceptar y firmar los términos y condiciones de su contrato de trabajo, que debe establecer sus responsabilidades y las de la or- ganización en lo relativo a seguridad de la información. |
| ***A.8.2 Durante el empleo****Objetivo:* Asegurar que todos los empleados, contratistas y terceros son conscientes de las amenazas y problemas que afectan a la seguridad de la información y de sus responsabilidades y obligaciones, y de que están preparados para cumplir la política de seguridad de la organización, en el desarrollo habitual de su trabajo, y para reducir el riesgo de error humano. |
| **No implementado** | Responsabilidades de la Dirección | *Control* La Dirección debe exigir a los empleados, con- tratistas y terceros, que apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos en la organización. |
| **No implementado** | Concienciación, formación y capacitación en seguridad de la información | *Control* Todos los empleados de la organización y, cuando corresponda, los contratistas y terceros, deben recibir una adecuada concienciación y formación, con actualizaciones periódicas, sobre las políticas y procedimientos de la orga- nización, según corresponda con su puesto de trabajo. |

|  |  |  |
| --- | --- | --- |
| **No implementado** | Proceso disciplinario | *Control* Debe existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad. |
| ***A.8.3 Cese del empleo o cambio de puesto de trabajo****Objetivo:* Asegurar que los empleados, contratistas y terceros abandonan la organización o cambian de puesto de trabajo de una manera ordenada. |
| **Implementado** | Responsabilidad del cese o cambio | *Control* Las responsabilidades para proceder al cese en el empleo o al cambio de puesto de trabajo deben estar claramente definidas y asignadas. |
| **Implementado** | Devolución de activos | *Control* Todos los empleados, contratistas y terceros de- ben devolver todos activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo. |
| **Implementado** | Retirada de los derechos de acceso | *Control* Los derechos de acceso a la información y a los recursos de tratamiento de la información de todos los empleados, contratistas y terceros deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o bien deben ser adaptados a los cambios producidos |
| **A.9 Seguridad física y ambiental** |
| ***A.9.1 Áreas seguras****Objetivo:* Prevenir los accesos físicos no autorizados, los daños y las intromisiones en las instalaciones y en la información de la organización. |
| **Implementado** | Perímetro de seguridad física | *Control* Se deben utilizar perímetros de seguridad (barreras, muros, puertas de entrada con control a través de tarjeta, o puestos de control) para proteger las áreas que contienen la información y los recursos de tratamiento de la información. |
| **Implementado** | Controles físicos de entrada | *Control* Las áreas seguras deben estar protegidas por controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado. |
| **Implementado** | Seguridad de oficinas, despachos e instalaciones | *Control* Se deben diseñar y aplicar las medidas de se- guridad física para las oficinas, despachos e instalaciones. |
| **Implementado** | Protección contra las amenazas externas y de origen ambiental | *Control* Se debe diseñar y aplicar una protección física contra el daño causado por fuego, inundación, terremoto, explosión, revueltas sociales y otras formas de desastres naturales o provocados por el hombre. |
| **Implementado** | Trabajo en áreas seguras | *Control* Se deben diseñar e implantar una protección física y una serie de directrices para trabajar en las áreas seguras. |
| **No implementado** | Áreas de acceso público y de carga y descarga | *Control* Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, a través de los que personal no autorizado puede acceder a las instalaciones, y si es posible, dichos puntos se deben aislar de los recursos de tratamiento de la información para evitar los accesos no autorizados. |
| ***A.9.2 Seguridad de los equipos****Objetivo:* Evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos, o que puedan provocar la interrupción de las actividades de la organización. |
| **No implementado** | Emplazamiento y protección de equipos | *Control* Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos derivados de las amenazas y peligros de origen ambiental así como las ocasiones de que se produzcan accesos no autorizados. |
| **Implementado** | Instalaciones de suministro | *Control* Los equipos deben estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro. |
| **No implementado** | Seguridad del cableado | *Control* El cableado eléctrico y de telecomunicaciones que transmite datos o que da soporte a los servicios de información debe estar protegido frente a interceptaciones. |
| **implementado** | Mantenimiento de los equipos | *Control* Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad. |
| **No implementado** | Seguridad de los equipos fuera de las instalaciones | *Control* Teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de las instalaciones de la organización, deben aplicarse medidas de seguridad a los equipos situados fuera dichas instalaciones. |
| **No implementado** | Reutilización o retirada segura de equipos | *Control* Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y todas las licencias de software se han eliminado o bien se han recargado de manera segura, antes de su retirada. |
| **No implementado** | Retirada de materiales propiedad de la empresa | *Control* Los equipos, la información o el software no deben sacarse de las instalaciones, sin una autorización previa. |
| **A.10 Gestión de comunicaciones y operaciones** |
| ***A.10.1 Responsabilidades y procedimientos de operación****Objetivo:* Asegurar el funcionamiento correcto y seguro de los recursos de procesamiento de la información. |
| **No implementado** | Documentación de los procedimientos de operación | *Control* Deben documentarse y mantenerse los procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten. |
| **Implementado** | Gestión de cambios | *Control* Deben controlarse los cambios en los recursos y los sistemas de tratamiento de la información. |
| **No implementado** | Segregación de tareas | *Control* Las tareas y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización. |
| **No implementado** | Separación de los recursos de desarrollo, prueba y operación | *Control* Deben separarse los recursos de desarrollo, de pruebas y de operación, para reducir los riesgos de acceso no autorizado o los cambios en el sistema operativo. |
| ***A.10.2 Gestión de la provisión de servicios por terceros****Objetivo:* Implantar y mantener el nivel apropiado de seguridad de la información en la provisión del servicio, en con- sonancia con los acuerdos de provisión de servicios por terceros. |
| **Implementado** | Provisión de servicios | *Control* Se debe comprobar que los controles de seguridad, las definiciones de los servicios y los niveles de provisión, incluidos en el acuerdo de provisión de servicios por terceros, han sido implantados, puestos en operación y son mantenidos por parte de un tercero. |

|  |  |  |
| --- | --- | --- |
| **Implementado** | Supervisión y revisión de los servicios prestados por terceros | *Control* Los servicios, informes y registros proporciona- dos por un tercero deben ser objeto de supervisión y revisión periódicas, y también deben llevarse a cabo auditorias periódicas. |
| **Implementado** | Gestión de cambios en los servicios prestados por terceros | *Control* Se deben gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y los controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas del negocio afectados así como la reevaluación de los riesgos. |
| ***A.10.3 Planificación y aceptación del sistema****Objetivo:* Minimizar el riesgo de fallos de los sistemas. |
| **No implementado** | Gestión de capacidades | *Control* La utilización de los recursos se debe supervisar y ajustar así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el comportamiento requerido del sistema. |
| **No implementado** | Aceptación del sistema | *Control* Se deben establecer los criterios para la aceptación de nuevos sistemas de información, de las actualizaciones y de nuevas versiones de los mismos, y se deben llevar a cabo pruebas adecuadas de los sistemas durante el desarrollo y previamente a la aceptación. |
| ***A.10.4 Protección contra código malicioso y descargable****Objetivo:* Proteger la integridad del software y de la información. |
| **No implementado** | Controles contra el código malicioso | *Control* Se deben implantar los controles de detección, prevención y recuperación que sirvan como protección contra código malicioso y se deben implantar procedimientos adecuados de concienciación del usuario. |
| **Implementado** | Controles contra el código descargado en el cliente | *Control* Cuando se autorice el uso de código descargado en el cliente, (JavaScript, VBScript, applets de Java applets, controles ActiveX, etc..), la configuración debe garantizar que dicho código autorizado funciona de acuerdo con una política de seguridad claramente definida, y se debe evitar que se ejecute el código no autorizado. |
| ***A.10.5 Copias de seguridad****Objetivo:* Mantener la integridad y disponibilidad de la información y de los recursos de tratamiento de la información. |
| **Implementado** | Copias de seguridad de la información | *Control* Se deben realizar copias de seguridad de la información y del software, y se deben probar periódicamente con conforme a la política de copias. |
| ***A.10.6 Gestión de la seguridad de las redes****Objetivo:* Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte. |
| **Implementado** | Controles de red | *Control* Las redes deben estar adecuadamente gestionadas y controladas, para que estén protegidas frente a posibles amenazas y para mantener la seguridad de los sistemas y de las aplicaciones que utilizan estas redes, incluyendo la información en tránsito. |

|  |  |  |
| --- | --- | --- |
| **Implementado** | Seguridad de los servicios de red | *Control* Se deben identificar las características de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en todo acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan. |
| ***A.10.7 Manipulación de los soportes****Objetivo:* Evitar la revelación, modificación, retirada o destrucción no autorizada de los activos, y la interrupción de las actividades de la organización. |
| **Implementado** | Gestión de soportes extraíbles | *Control* Se deben establecer procedimientos para la gestión de los soportes extraíbles. |
| **No implementado** | Retirada de soportes | *Control* Los soportes deben ser retirados de forma segura cuando ya no vayan a ser necesarios, mediante los procedimientos formales establecidos. |
| **No implementado** | Procedimientos de manipulación de la información | *Control* Deben establecerse procedimientos para la manipulación y el almacenamiento de la información, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido. |
| **Implementado** | Seguridad de la documentación del sistema | *Control* La documentación del sistema debe estar protegida contra accesos no autorizados. |
| ***A.10.8 Intercambio de información****Objetivo:* Mantener la seguridad de la información y del software intercambiados dentro de una organización y con un tercero |
| **No implementado** | Políticas y procedimientos de intercambio de información | *Control* Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación. |
| **No implementado** | Acuerdos de intercambio | *Control* Deben establecerse acuerdos para el intercambio de información y del software entre la organización y los terceros. |
| **No implementado** | Soportes físicos en tránsito | *Control* Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro. |
| **Implementado** | Mensajería electrónica | *Control* La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida. |
| **No implementado** | Sistemas de información empresariales | *Control* Deben formularse e implantarse políticas y procedimientos para proteger la información asociada a la interconexión de los sistemas de información empresariales |
| ***A.10.9 Servicios de comercio electrónico****Objetivo:* Garantizar la seguridad de los servicios de comercio electrónico, y el uso seguro de los mismos |
| **Implementado** | Comercio electrónico | *Control* La información incluida en el comercio electrónico que se transmita a través de redes públicas debe protegerse contra las actividades fraudulentas, las disputas contractuales, y la revelación o modificación no autorizada de dicha información. |

|  |  |  |
| --- | --- | --- |
| **No implementado** | Transacciones en línea | *Control* La información contenida en las transacciones en línea debe estar protegida para evitar transmisiones incompletas, errores de direccionamiento, alteraciones no autorizadas de los mensajes, la revelación, la duplicación o la reproducción no autorizadas del mensaje. |
| **Implementado** | Información puesta a disposición pública | *Control* La integridad de la información puesta a disposición pública se debe proteger para evitar modificaciones no autorizadas. |
| ***A.10.10 Supervisión****Objetivo:* Detectar las actividades de procesamiento de la información no autorizadas. |
| **Implementado** | Registro de auditorias | *Control* Se deben realizar registros de auditoria de las actividades de los usuarios, las excepciones y eventos de seguridad de la información, y se deben mantener estos registros durante un periodo acordado para servir como prueba en investigaciones futuras y en la supervisión del control de acceso. |
| **No implementado** | Supervisión del uso del sistema | *Control* Se deben establecer procedimientos para supervisar el uso de los recursos de procesamiento de la información y se deben revisar periódicamente los resultados de las actividades de supervisión. |
| **No implementado** | Protección de la información de los registros | *Control* Los dispositivos de registro y la información de los registros deben estar protegidos contra manipulaciones indebidas y accesos no autorizados. |
| **Implementado** | Registros de administración y operación | *Control* Se deben registrar las actividades del administrador del sistema y de la operación del sistema. |
| **Implementado** | Registro de fallos | *Control* Los fallos deben ser registrados y analizados y se deben tomar las correspondientes acciones |
| **Implementado** | Sincronización del reloj | *Control* Los relojes de todos los sistemas de procesamiento de la información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una precisión de tiempo acordada. |
| ***A.11 Control de acceso*** |
| ***A.11.1 Requisitos de negocio para el control de acceso****Objetivo:* Controlar el acceso a la información |
| **No implementado** | Política de control de acceso | *Control* Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos empresariales y de seguridad para el acceso. |
| ***A.11.2 Gestión de acceso de usuario****Objetivo:* Asegurar el acceso de un usuario autorizado y prevenir el acceso no autorizado a los sistemas de información |
| **Implementado** | Registro de usuario | *Control* Debe establecerse un procedimiento formal de registro y de anulación de usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información. |
| **Implementado** | Gestión de privilegios | *Control* La asignación y el uso de privilegios deben estar restringidos y controlados. |
| **Implementado** | Gestión de contraseñas de usuario | *Control* La asignación de contraseñas debe ser controlada a través de un proceso de gestión formal |

|  |  |  |
| --- | --- | --- |
| **No implementado** | Revisión de los derechos de acceso de usuario | *Control* La Dirección debe revisar los derechos de acceso de usuario a intervalos regulares y utilizando un proceso formal. |
| ***A.11.3 Responsabilidades de usuario****Objetivo:* Prevenir el acceso de usuarios no autorizados, así como evitar el que se comprometa o se produzca el robo de la información o de los recursos de procesamiento de la información |
| **No implementado** | Uso de contraseña | *Control* Se debe requerir a los usuarios el seguir las buenas prácticas de seguridad en la selección y el uso de las contraseñas. |
| **Implementado** | Equipo de usuario desatendido | *Control* Los usuarios deben asegurarse de que el equipo desatendido tiene la protección adecuada. |
| **No implementado** | Política de puesto de trabajo despejado y pantalla limpia | *Control* Debe adoptarse una política de puesto de trabajo despejado de papeles y de soportes de almacenamiento extraíbles junto con una política de pantalla limpia para los recursos de procesamiento de la información. |
| ***A.11.4 Control de acceso a la red****Objetivo:* Prevenir el acceso no autorizado a los servicios en red. |
| **Implementado** | Política de uso de los servicios en red | *Control* Se debe proporcionar a los usuarios únicamente el acceso a los servicios para que los que hayan sido específicamente autorizados. |
| **Implementado** | Autenticación de usuario para conexiones externas | *Control* Se deben utilizar los métodos apropiados de autenticación para controlar el acceso de los usuarios remotos. |
| **Implementado** | Identificación de los equipos en las redes | *Control* La identificación automática de los equipos se debe considerar como un medio de autenticación de las conexiones provenientes de localizaciones y equipos específicos. |
| **Implementado** | Diagnóstico remoto y protección de los puertos de configuración | *Control* Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y de configuración. |
| **Implementado** | Segregación de las redes | *Control* Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en redes. |
| **Implementado** | Control de la conexión a la red | *Control* En redes compartidas, especialmente en aquellas que traspasen las fronteras de la organización, debe restringirse la capacidad de los usuarios para conectarse a la red, esto debe hacerse de acuerdo a la política de control de acceso y a los requisitos de las aplicaciones del negocio (véase 11.1). |
| **Implementado** | Control de encaminamiento (*routing)* de red | *Control* Se deben implantar controles de encaminamiento (*routing*) de redes para asegurar que las conexiones de los ordenadores y los flujos de información no violan la política de control de acceso de las aplicaciones empresariales. |
| ***A.11.5 Control de acceso al sistema operativo****Objetivo:* Prevenir el acceso no autorizado a los sistemas operativos. |
| **Implementado** | Procedimientos seguros de inicio de sesión | Control El acceso a los sistemas operativos se debe controlar por medio de un procedimiento seguro de inicio de sesión. |

|  |  |  |
| --- | --- | --- |
| **Implementado** | Identificación y autenticación de usuario | *Control* Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal y exclusivo, y se debe elegir una técnica adecuada de autenticación para confirmar la identidad solicitada del usuario. |
| **Implementado** | Sistema de gestión de contraseñas | *Control* Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas. |
| **No implementado** | Uso de los recursos del sistema | *Control* Se debe restringir y controlar rigurosamente el uso de programas y utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación. |
| **Implementado** | Desconexión automática de sesión. | *Control* Las sesiones inactivas deben cerrarse después de un periodo de inactividad definido. |
| **Implementado** | Limitación del tiempo de conexión | *Control* Para proporcionar seguridad adicional a las aplicaciones de alto riesgo, se deben utilizar restricciones en los tiempos de conexión. |
| ***A.11.6 Control de acceso a las aplicaciones y a la información****Objetivo:* Prevenir el acceso no autorizado a la información que contienen las aplicaciones |
| **Implementado** | Restricción del acceso a la información | *Control* Se debe restringir el acceso a la información y a las aplicaciones a los usuarios y al personal de soporte, de acuerdo con la política de control de acceso definida. |
| **Implementado** | Aislamiento de sistemas sensibles | *Control* Los sistemas sensibles deben tener un entorno de ordenadores dedicados (aislados). |
| ***A.11.7 Ordenadores portátiles y teletrabajo****Objetivo:* Garantizar la seguridad de la información cuando se utilizan ordenadores portátiles y servicios de teletrabajo. |
| **No implementado** | Ordenadores portátiles y comunicaciones móviles | *Control* Se debe implantar una política formal y se deben adoptar las medidas de seguridad adecuadas de protección contra los riesgos de la utilización de ordenadores portátiles y comunicaciones móviles. |
| **No implementado** | Teletrabajo | *Control* Se debe redactar e implantar, una política de actividades de teletrabajo, así como los planes y procedimientos de operación correspondientes. |
| **A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información** |
| ***A.12.1 Requisitos de seguridad de los sistemas de información****Objetivo:* Garantizar que la seguridad está integrada en los sistemas de información. |
| **No implementado** | Análisis y especificación de los requisitos de seguridad | *Control* En las declaraciones de los requisitos de negocio para los nuevos sistemas de información, o para mejoras de los sistemas de información ya existentes, se deben especificar los requisitos de los controles de seguridad. |
| ***A.12.2 Tratamiento correcto de las aplicaciones****Objetivo:* Evitar errores, pérdidas, modificaciones no autorizadas o usos indebidos de la información en las aplicaciones |
| **No implementado** | Validación de los datos de entrada | *Control* La introducción de datos en las aplicaciones debe validarse para garantizar que dichos datos son correctos y adecuados. |
| **No implementado** | Control del procesamiento interno | *Control* Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deben incorporar comprobaciones de validación en las aplicaciones. |
| **No implementado** | Integridad de los mensajes | *Control* Se deben identificar los requisitos para garantizar la autenticidad y para proteger la integridad de los mensajes en las aplicaciones y se deben identificar e implantar los controles adecuados. |
| **No implementado** | Validación de los datos de salida | *Control* Los datos de salida de una aplicación se deben validar para garantizar que el tratamiento de la información almacenada es correcto y adecuado a las circunstancias. |
| ***A.12.3 Controles criptográficos****Objetivo:* Proteger la confidencialidad, la autenticidad o la integridad de la información por medios criptográficos. |
| **No implementado** | Política de uso de los controles criptográficos | *Control* Se debe formular e implantar una política para el uso de los controles criptográficos para proteger la información. |
| **No implementado** | Gestión de claves | *Control* Debe implantarse un sistema de gestión de claves para dar soporte al uso de técnicas criptográficas por parte de la organización. |
| ***A.12.4 Seguridad de los archivos de sistema****Objetivo:* Garantizar la seguridad de los archivos de sistema. |
| **Implementado** | Control del software en explotación | *Control* Deben estar implantados procedimientos para controlar la instalación de software en los sistemas operativos. |
| **Implementado** | Protección de los datos de prueba del sistema | *Control* Los datos de prueba se deben seleccionar con cuidado y deben estar protegidos y controlados. |
| **Implementado** | Control de acceso al código fuente de los programas | *Control* Se debe restringir el acceso al código fuente de los programas. |
| ***A.12.5 Seguridad en los procesos de desarrollo y soporte****Objetivo:* Mantener la seguridad del software y de la información de las aplicaciones |
| **Implementado** | Procedimientos de control de cambios | *Control* La implantación de cambios debe controlarse mediante el uso de procedimientos formales de control de cambios. |
| **Implementado** | Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo | *Control* Cuando se modifiquen los sistemas operativos, las aplicaciones empresariales críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o en la seguridad de la organización. |
| **Implementado** | Restricciones a los cambios en los paquetes de software | *Control* Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso. |
| **Implementado** | Fugas de información | *Control* Deben evitarse las situaciones que permitan que se produzcan fugas de información. |
| **Implementado** | Externalización del desarrollo de software | *Control* La externalización del desarrollo de software debe ser supervisado y controlado por la organización. |

|  |
| --- |
| ***A.12.6 Gestión de la vulnerabilidad técnica****Objetivo:* Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas. |
| **No implementado** | Control de las vulnerabilidades técnicas | *Control* Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información que están siendo utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado. |
| **A.13 Gestión de incidentes de seguridad de la información** |
| ***A.13.1 Notificación de eventos y puntos débiles de la seguridad de la información****Objetivo:* Asegurarse de que los eventos y las vulnerabilidades de la seguridad de la información, asociados con los sistemas de información, se comunican de manera que sea posible emprender las acciones correctivas oportunas. |
| **Implementado** | Notificación de los eventos de seguridad de la información | *Control* Los eventos de seguridad de la información se deben notificar a través de los canales adecuados de gestión lo antes posible. |
| **No implementado** | Notificación de los puntos débiles de la seguridad | *Control* Todos los empleados, contratistas, y terceros que sean usuarios de los sistemas y servicios de información deben estar obligados a anotar y notificar cualquier punto débil que observen o que sospechen exista, en dichos sistemas o servicios. |
| ***A.13.2 Gestión de incidentes de seguridad de la información y mejoras****Objetivo:* Garantizar que se aplica un enfoque coherente y efectivo a la gestión de los incidentes de seguridad de la información. |
| **Implementado** | Responsabilidades y procedimientos | *Control* Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información. |
| **Implementado** | Aprendizaje de los incidentes de seguridad de la información | *Control* Deben existir mecanismos que permitan cuantificar y supervisar los tipos, volúmenes y costes de los incidentes de seguridad de la información. |
| **No implementado** | Recopilación de evidencias | *Control* Cuando se emprenda una acción contra una persona u organización, después de un incidente de seguridad de la información, que implique acciones legales (tanto civiles como penales), deben recopilarse las evidencias, conservarse y presentarse conforme a las normas establecidas en la jurisdicción correspondiente. |
| **A.14 Gestión de la continuidad del negocio** |
| ***A.14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio****Objetivo:* Contrarrestar las interrupciones de las actividades empresariales y proteger los procesos críticos de negocio de los efectos derivados de fallos importantes o catastróficos de los sistemas de información, así como garantizar su oportuna reanudación |
| **No implementado** | Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio | *Control* Debe desarrollarse y mantenerse un proceso para la continuidad del negocio en toda la organización, que gestione los requisitos de seguridad de la información necesarios para la continuidad del negocio. |

|  |  |  |
| --- | --- | --- |
| **No implementado** | Continuidad del negocio y evaluación de riesgos | *Control* Deben identificarse los eventos que puedan causar interrupciones en los procesos de negocio, así como la probabilidad de que se produzcan tales interrupciones, sus efectos y sus consecuencias para la seguridad de la información. |
| **No implementado** | Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información | *Control* Deben desarrollarse e implantarse planes para mantener o restaurar las operaciones y garantizar la disponibilidad de la información en el nivel y en el tiempo requeridos, después de una interrupción o un fallo de los procesos de negocio críticos. |
| **No implementado** | Marco de referencia para la planificación de la continuidad del negocio | *Control* Debe mantenerse un único marco de referencia para los planes de continuidad del negocio, para asegurar que todos los planes sean coherentes, para cumplir los requisitos de seguridad de la información de manera consistente y para identificar las prioridades de realización de pruebas y de mantenimiento. |
| **No implementado** | Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio | *Control* Los planes de continuidad del negocio deben probarse y actualizarse periódicamente para asegurar que están al día y que son efectivos. |
| **A.15 Cumplimiento** |
| ***A.15.1 Cumplimiento de los requisitos legales****Objetivo:* Evitar incumplimientos de las leyes o de las obligaciones legales, reglamentarias o contractuales y de los requisitos de seguridad. |
| **No implementado** | Identificación de la legislación aplicable | *Control* Todos los requisitos pertinentes, tanto legales como reglamentarios o contractuales, y el enfoque de la organización para cumplir dichos requisitos, deben estar definidos, documentados y mantenerse actualizados de forma explícito para cada sistema de información de la organización. |
| **Implementado** | Derechos de propiedad intelectual (DPI) [*Intellectual Property Rights* (IPR)] | *Control* Deben implantarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso de material, con respecto al cual puedan existir derechos de propiedad intelectual y sobre el uso de productos de software/propietario. |
| **No implementado** | Protección de los documentos3) de la organización | *Control* Los documentos importantes deben estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, regulatorios, contractuales y empresariales. |
| **Implementado** | Protección de datos y privacidad de la información personal | *Control* Debe garantizarse la protección y la privacidad de los datos según se requiera en la legislación y las regulaciones y, en su caso, en las cláusulas contractuales pertinentes. |
| **Implementado** | Prevención del uso indebido de los recursos de tratamiento de la información | *Control* Se debe impedir que los usuarios utilicen los recursos de tratamiento de la información para fines no autorizados. |

|  |  |  |
| --- | --- | --- |
| **No implementado** | Regulación de los controles criptográficos | *Control* Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes. |
| ***A.15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico****Objetivo:* Asegurar que los sistemas cumplen las políticas y normas de seguridad de la organización. |
| **No implementado** | Cumplimiento de las políticas y normas de seguridad | *Control* Los directores deben asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad. |
| **No implementado** | Comprobación del cumplimiento técnico | *Control* Debe comprobarse periódicamente que los sistemas de información cumplen las normas de aplicación de la seguridad. |
| ***A.15.3 Consideraciones sobre la auditoria de los sistemas de información****Objetivo:* Lograr que el proceso de auditoría de los sistemas de información alcance la máxima eficacia con las mínimas interferencias. |
| **No implementado** | Controles de auditoria de los sistemas de información | *Control* Los requisitos y las actividades de auditoria que impliquen comprobaciones en los sistemas operativos de- ben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de empresariales. |
| **No implementado** | Protección de las herramientas de auditoria de los sistemas de información | *Control* El acceso a las herramientas de auditoria de los sistemas de información debe estar protegido para evitar cualquier posible peligro o uso indebido. |

***5.5 Conclusiones***

Al realizar la comprobación de los controles de la norma implantados en la empresa, determinamos el estado de madurez en la que se encuentra la organización, dicho estado de madurez bajo, posee un nivel adecuado de uso de redes pero por lo contrario el uso de políticas de protección de datos y material sensible es relativamente bajo.

6 Red y medidas de seguridad

La empresa ya contiene unas pautas para preservar la confidencialidad, exactitud y disponibilidad de la información conforme a la 27001 así que se realizarán pequeñas mejoras para un futuro.

***6.1 Mapa de red***



***6.2 Documento de confidencialidad***

Los empleados firmaran un acuerdo de confidencialidad en el que se comprometerán a mantener y proteger la privacidad e integridad de los datos.

Ver ANEXO 1.

***6.3 Cuentas de usuarios***

Los usuarios deberán estar dados de alta en el servidor para poder utilizar el sistema de información implantado en la organización.

Los datos que se ingresaran en la cuenta son los siguientes.

• ID usuario: El identificador será único para cada usuario este estará formado por las dos primeras letras de su nombre, las dos primeras de su primer apellido y las dos primeras de su segundo apellido. Al final del identificador aparecerá un número que nos indicara a que unidad organizativa pertenece dicho usuario. Si ocurriera que coinciden dos personas con el mismo identificador se añadiría otro número detrás del de la Unidad organizativa siguiendo un orden lógico.

El ID de usuario será de la siguiente forma

|  |  |
| --- | --- |
| NOMBRE | ID |
| Jorge Anduix Fuentes | Joranfue |

***6.4 Autentificación***

En la pantalla de login de los sistemas se mostrarán los siguientes datos:

• Nombre de usuario

• Password

• Posibilidad cambiar password

Cuando el usuario ingrese su password en el sistema, aparecerán asteriscos en lugar del password introducido, si el usuario se logea incorrectamente 5 veces la cuenta se bloqueara hasta que el usuario se ponga en contacto con el administrador del sistema.

Una vez el usuario se ha logreado aparece en pantalla el nombre del usuario.

En la organización se utiliza la firma digital para el envío de información confidencial con la administración pública.

Se utilizará la firma digital para enviar cualquier email que contenga datos de carácter personal de cualquier cliente o trabajador.

***6.5 Passwords***

Los passwords que existen en la empresa se generaran de forma manual, sin procedimientos automáticos, tanto el inicial, como el puesto por el usuario.

Inicialmente será el ID de usuario, cuando el usuario acceda por primera vez al sistema se le obligara a cambiar la contraseña acorde a las políticas de seguridad de la empresa.

El sistema a los cada 60 días enviará un mensaje al usuario para su contraseña impidiendo que pueda repetir su contraseña actual.

Si un usuario introduce 5 veces su password incorrectamente el usuario se bloqueará, para volver a activar la cuenta deberá comunicárselo al administrador.

***6.6 Permisos a la base de datos***

Deben asignarse los permisos mínimos y necesarios para que cada usuario desempeñe su tarea.

***6.7 Inactividad***

Cuando el usuario permanezca más de 5 minutos sin actividad la sesión se bloqueará automáticamente.

7 Políticas de seguridad de la información

***7.1 Políticas de seguridad para equipos y empleados***

La información sobre cualquier cliente se considera confidencial. En ningún caso debe revelarse a ninguna persona ajena a la empresa.

• Toda persona que necesite utilizar el sistema recibirá un ID de usuario y una contraseña. Se le solicitará que cambie su contraseña la primera vez que inicie la sesión en el sistema y cada 60 días a partir de ese momento. Elija una contraseña que pueda recordar, pero que no sea fácil de adivinar

• Las contraseñas no podrán ser fechas de cumpleaños, nombres de personas, números de teléfono, palabras de diccionario, es decir, datos que se puedan relacionar con usted. La contraseña dispondrá de 10 caracteres para los usuarios y 20 para el servidor. Las dos deben contener mayúsculas y minúsculas, números, letras y caracteres especiales.

• No comparta su contraseña con nadie. Nuestra intención es que pueda llevar a cabo todas las tareas en el sistema que sean necesarias para su trabajo. Si necesita acceder a determinada información, póngase en contacto con el administrador de red. Si olvida su contraseña, puede configurarle una contraseña nueva de inmediato. No hay ningún motivo para que una persona inicie la sesión con el ID de usuario y la contraseña de otra.

• No grabe su contraseña en el PC para copiarla y pegarla.

• Si apunta en un papel la contraseña este debe estar en un lugar seguro donde NADIE pueda acceder a él.

• No abandone la estación de trabajo con la sesión iniciada cuando no esté en su escritorio. En la formación ha aprendido a finalizar la sesión de la estación de trabajo de forma temporal. Utilice esta función si tiene que abandonar el escritorio durante un período de tiempo breve. Si va a estar ausente durante un período largo, termine el trabajo y utilice el procedimiento de fin de sesión normal.

• Cuando un usuario no realice ninguna acción en 10 minutos la sesión se cerrara automáticamente.

• Cuando un usuario introduzca 5 veces su password erróneamente la cuenta se bloqueara hasta que el administrador de la red hable con el usuario afectado.

• Está completamente prohibido sacar información confidencial de la organización sin permiso firmado del gerente y únicamente para fines relacionados con el trabajo.

• Si es necesario extraer información de la empresa esta estará cifrada para evitar acceso a la información en caso de pérdida o robo.

• Cuando la información sea cifrada el responsable de seguridad dará su permiso para sacar la información de la empresa.

• Los accesos por medio de almacenamiento extraíbles a la computadora serán desactivados, solamente podrán ser utilizados con el permiso del gerente, se presentara un escrito en el que aparezca para que se quiere utilizar y durante cuánto tiempo, este deberá ser firmado por el gerente.

• El usuario entregará la autorización al administrador de la red que dará permiso al usuario según las premisas marcadas.

• Cada usuario únicamente tendrá acceso a la información que sea necesaria para desarrollar su tarea dentro de la empresa. El gerente de la organización junto con el administrador de red decidirá el acceso de los usuarios a la información.

• No utilice redes sociales en su estación de trabajo.

• No utilizar programas de descarga P2P.

• No descargue programas, archivos...de Internet sino proviene de una fuente segura.

• No abra correos de personas desconocidas para usted, ni descargue archivos adjuntos.

• Solamente se dispondrá de acceso a Internet en las páginas necesarias para desempeñar su trabajo.

 • No utilice programas de mensajería instantánea como Messenger.

• El sistema operativo solo dispondrá de lo estrictamente necesario para realizar las tareas referentes al trabajo

• Todos los equipos dispondrán de un antivirus corporativo.

Recuerde que nuestro sistema pretende facilitar el trabajo y mejorar el rendimiento de la empresa. Las políticas de seguridad adoptadas están concebidas para ayudarle, no para obstaculizar su trabajo. Si desea plantear alguna pregunta o cuestión al respecto, no dude en ponerse en contacto con el administrador de red.

***7.2 Políticas de seguridad para router***

• Utilizar servidor RADIUS

•Filtrar por MAC los dispositivos conectados por red.

• Cambiar la contraseña por defecto.

• Cerrar los puertos innecesarios.

• Ocultar SSID.

• Desactivación del DHCP del router.

***7.3 Políticas de seguridad para servidor***

• Únicamente tendrá acceso al servidor el administrador y responsable de la red con el fin de mantener la consistencia con las políticas de seguridad.

• Únicamente se instalaran en el servidor los servicios y aplicaciones estrictamente necesarias.

• El acceso a los servicios que proporciona el servidor, deberá ser registrado en un Log.

• Se deberán instalar las últimas actualizaciones de seguridad en el momento que no interfiera con la demanda de trabajo.

• No realizar la cuenta de administrador para realizar operaciones que pueden ser hechas por cualquier otro usuario.

• Cambiar puertos estándar, asignar a los servicios puertos altos.

• Cifrar las conexiones de red mediante SSH o IPSec.

• Todos los registros relacionados con la seguridad del equipo deberán ser guardados por un periodo mínimo de un mes.

• Las copias incrementales realizadas día a día deberán ser almacenadas al menos un mes.

• Las copias totales realizadas cada semana deberán ser almacenadas por lo menos un mes.

• Las copias totales realizadas cada mes, deberán ser almacenadas por lo menos dos años.

• Todos los eventos de seguridad deberán ser informados al gerente de la empresa y responsable de seguridad. Las medidas correctivas se aplicaran según las necesidades.

• Todos los eventos de seguridad deberán incluir:

 Ataque de escaneo de puertos.

 Evidencias de acceso no autorizado a cuentas privilegiadas.

 Eventos sospechosos que posiblemente no estarán relacionados con aplicaciones instaladas en el equipo.

• Los usuarios dispondrán de una cuota de disco de 4 GB.

• Debe existir únicamente dos cuentas de administrador del sistema operativo en los equipos o servidores.

• Es necesario la utilización de firewall para detección de intrusos, este sistema será controlado por el administrador de la red y responsable de seguridad, deberá incluir un Log que registre intentos de acceso autorizados y no autorizados.

• El responsable del servidor no debe escribir ni colocar la contraseña de la cuenta de administración y configuración del sistema de seguridad en lugares donde pueda ser descubierta por otras personas.

• El servidor y los PC’s dispondrán de una IP fija.

• Las auditorías internas serán administradas por el responsable de seguridad, se presentarán los resultados al gerente y se le plantearan las soluciones, la auditoria se realizara cada trimestre.

• Todas las conexiones externas hacia el servidor se realizaran mediante VPN y se cifrara la conexión.

• Cualquier persona que viole estas políticas será sancionado de acuerdo con los criterios establecidos por el gerente y responsable de seguridad.

***7.4 Políticas de seguridad para BBDD***

• Para Mantener la confidencialidad de los datos los usuarios se logearan en el servidor para acceder en la base de datos.

• Todas las acciones realizadas sobre la base de datos serán monitorizadas para evitar robo y fraude en la información confidencial que esta contiene.

• Los usuarios solamente podrán acceder a la información estrictamente necesaria para desempeñar su trabajo.

• No se podrá sacar datos de la empresa a excepción de que sea mediante las condiciones expuestas en el punto 1 (políticas de seguridad para equipos y empleados)

• Se realizaran copias de seguridad de la base de datos incrementales todos los días deberán ser almacenadas un mes.

• Se realizaran copias de seguridad totales todas las semanas deberán ser almacenadas durante un mes.

• Se realizaran copias totales todos los meses que deberán ser almacenadas durante 2 años.

• Para mantener la integridad y disponibilidad de nuestra base de datos utilizaremos RAID 1.

• Todos los datos que se encuentran en formato papel deberán ser almacenadas en armarios especiales con cierre de seguridad.

• La base de datos se inscribirá en la agencia de protección de datos para el cumplimiento de la LOPD.

***7.5 Políticas de seguridad para Correo electrónico***

• Cada usuario dispondrá de una cuota de correo de 300MB.

• Cada semana se eliminaran automáticamente los mensajes que se encuentren en la papelera.

• No se podrán enviar mensajes en cadena a múltiples usuarios, ya se enviando o reenviando este tipo de mensajes.

• El administrador no podrá interceptar, editar, monitorear o eliminar ningún mensaje de correo de ningún usuario con las siguientes excepciones:

- El usuario haya incurrido en actos ilegales

- Requerimiento expreso de autoridades judiciales o policiales

- Para identificar o resolver problemas técnicos

- El mensaje comprometa el normal funcionamiento del servicio

• La contraseña es secreta e individual no deberá ser confiada a ninguna otra persona

• No descargue archivos adjuntos de personas desconocidas

• Para reforzar una política anti-virus y anti-spam, todo correo recibido pasara unos filtros por una serie de filtros

• Se realizara una copia de seguridad del correo electrónico una vez por semana guardando esta durante 1 año.

***7.6 Políticas de seguridad para Backups***

• Se realizarán copias de seguridad de todos los archivos incrementales todos los días deberán ser almacenadas un mes.

• Se realizarán copias de seguridad totales todas las semanas deberán ser almacenadas durante un mes.

• Se realizarán copias totales todos los meses que deberán ser almacenadas durante 2 años.

• Se realizará una copia de seguridad del correo electrónico una vez por semana guardando esta durante 1 año.

• Las copias de seguridad se almacenarán en el servidor de la organización, también se realizara una copia en un disco duro externo con capacidad de 1 ́5 TB, ha este disco duro solo podrá acceder el administrador de red, esta unidad estará oculta para cualquier usuario.

• No se realizarán copias de seguridad de los datos privados de los empleados, solamente de los datos almacenados en el servidor.

• Los backups de los que disponga la organización antes de la implantación del SGSI serán guardadas en una caja fuerte a la que solamente tendrá acceso el gerente de la organización.

8 Organización de la seguridad de la información

***8.1 Asignación responsabilidades***

Gerente de la empresa:

• Será el responsable de supervisar que el SGSI se aplica correctamente por parte de los usuarios y el mismo.

• Si existe algún indicio o sospecha de que no se está cumpliendo el SGSI en la organización por parte de algún empleado el gerente avisará inmediatamente al responsable de seguridad de la organización.

***8.2 Responsabilidad por los activos***

Objetivo: Lograr y mantener la protección apropiada de los activos organizacionales.

***8.3 Clasificación de la información***

Objetivo: Asegurar que la información reciba un nivel de protección apropiado

Para asegurarnos que la información de la organización recibe un nivel de protección apropiado la organización se aplicará a parte de la seguridad incluida en el sistema, como firewall, acceso restringido, copias de seguridad...se dará de alta en la agencia española de protección de datos la base de datos de la empresa para el cumplimiento de la LOPD, clasificando la información según esta ley.

***8.4 Seguridad de los recursos humanos***

Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera y reducir el riesgo de robo, fraude y mal uso de los medios.

Los empleados firmaran un documento en el que se comprometen a mantener la confidencialidad de los datos que manejan

Anexo 1 y 3.

***8.5 Seguridad física y ambiental***

Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.

El CPD dispone de una puerta blindada protegida con pin y llave, también dispone de extracción de humos y extinción de fuegos mediante CO2.

***8.6 Control de acceso a equipos***

Todos los equipos disponen de lector/grabador de DVD y puertos usb habilitados, ya que son necesarios para desarrollar su trabajo.

Cualquier acceso a PC’s será realizado mediante el usuario previamente creado el cual poseerá unos u otros permisos en función del tipo de usuario.

Se realizarán controles periódicos de hardware instalados en los equipos, para evitar que se instalen o desinstalen dispositivos.

El servidor no se apagara nunca, exceptuando alguna noche para realizar tareas de mantenimiento.

***8.7 Transporte***

La empresa tiene externalizada los servicios de transporte por lo que la empresa contratada ofrece un servicio de tracking para el seguimiento de los envíos.

9 Protección contra Malware

Objetivo: Proteger la integridad del software y la información

***9.1 Antivirus***

La empresa dispone de una versión corporativa de Panda Antivirus, de manera que en el servidor existe una versión instalada para este y en el resto de los equipos una versión de AVG antivirus.

El antivirus está ejecutándose continuamente y se actualiza todos los días por la noche. Los escaneos de virus se deben realizará una vez por semana en cada PC y todos los días en el servidor.

 ***9.2 Malware***

Se utilizan las herramientas malwarebyte, combofix y spybot search and destroy para controlar si existe malware y software espía en el equipo, el proceso de escaneo se realiza dos veces al mes.

 ***9.3 Firewall***

Se ha configurado de manera que se prohíben todos los servicios y solo se habilitan los necesarios.

Se ha configurado en base a una política que discrimina tres clases de paquetes de red:

• Los paquetes entrantes a la red

• Los paquetes salientes de la red

• Los paquetes en transito

Por defecto, lo que no se habilite explícitamente está prohibido. Se les denegara el acceso a todos los paquetes de entrada y a los paquetes en tránsito, mientras que a los de salida se les permite la salida.

* Se aceptan todos los paquetes que van y vienen de la red interna.

Los servicios o protocolos que solo sean necesarios esporádicamente deberán habilitarse bajo demanda.

***9.4 Ataques de red***

Toda la información que se considere confidencial deberá encriptarse durante la transmisión, o viajar en formato no legible.

***9.5 Web***

La creación y el mantenimiento de la web están subcontratado a una empresa.

10 Gestión de seguridad de redes

**Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte**

El esquema de direcciones de la red interna no será visible ante las conexiones externas.

Se controlara el número de conexiones externas ya que la conectividad debe ser la mínima.

TODO lo que suceda en la red será visible en el Log del sistema y en las aplicaciones utilizadas para el monitoreo de este.

Los logs se revisaran una vez a la semana para comprobar si ha ocurrido algo extraño en nuestra red.

Si ocurre un fallo de seguridad se registrará y se analizara para tomar la decisión apropiada para la solución de este fallo.

11 Gestión de riesgos

***11.1 Análisis de riesgos***

El análisis de riesgos intenta contestar a las siguientes preguntas:

• ¿Qué puede salir mal?

• ¿Qué probabilidad hay de que algo salga mal?

• ¿Cuáles pueden ser las consecuencias de que algo salga mal?

• ¿Qué se puede hacer para reducir la probabilidad y las consecuencias de que algo salga mal?

El siguiente análisis de riesgos se desarrolla para determinar cuáles de los activos de la organización tienen mayores vulnerabilidades ante factores internos y externos, identificando las causas que facilitan o impiden alcanzar los objetivos, calculando la probabilidad de ocurrencia, evaluando los efectos y considerando el grado en que el riesgo puede ser controlado.

Para realizar el análisis de riesgo se siguen las siguientes pautas.

 Listar los activos de la empresa

El activo esencial es la información que maneja el sistema, es decir, los datos. Y alrededor de estos datos se identifican los demás activos relevantes.

* Los servicios que se pueden prestar gracias a los datos, y los servicios que se necesitan para gestionarlos.
* Las aplicaciones informáticas (software) que permiten manejar los datos.
* Los equipos informáticos (Hardware) que permiten hospedar datos, aplicaciones y servicios.
* Los soportes de información que son dispositivos de almacenamientos de datos
* El equipamiento auxiliar que complementa el material informático.
* Las redes de comunicaciones que permiten intercambiar datos.
* Las instalaciones que acogen equipos informáticos y de comunicaciones.
* Las personas que explotan u operan todos los elementos anteriores citados.

 Asignación de prioridades a los activos

Clasificare los activos según el impacto que sufrirá la organización si faltase o fallara dicho activo.

 Definición de los factores de riesgo

Se listan los factores de riesgo relevantes que pueden afectar a cada uno de los activos

 Descripción de consecuencias

Se genera una descripción de consecuencias que podría sufrir la empresa si los activos son afectados por sus factores de riesgo, detallando la manera en que se protege el activo contra ese ataque particular y puntualizando el nivel de efectividad de las medidas.

 Asignación de probabilidades de ocurrencia de los factores de riesgo

Teniendo en cuenta la descripción de consecuencias se estima la probabilidad de ocurrencia que cada uno de los factores de riesgo representa con respecto a los activos de la empresa, considerando las medidas tomadas por la empresa para reducir la acción.

 Cálculo de niveles de vulnerabilidad

Una vez identificados los riesgos se realiza el análisis. Con toda la información obtenida se determina el nivel de vulnerabilidad de cada activo.

 Conclusiones

A partir de los puntos anteriores se evalúa la situación actual de la empresa en relación a los incidentes que pueden afectarla, se calcula el porcentaje de los riesgos cubiertos y descubiertos, y se realiza un análisis sobre la escala de importancia de los activos.

 Consecuencias

Tras identificar, estimar y cuantificar los riesgos, el gerente de la empresa determina los objetivos específicos de control, y con relación a ellos se establecen los procedimientos de control para afrontarlos de la manera más eficaz y económica posible.

 ***11.2 Activos y factores de riesgos***

Aquí se muestran los activos que tiene nuestra organización, se asigna un valor según la importancia que tiene dentro de la organización, esta valoración la realizare con valores del 1 al 10.

Este es un valor subjetivo que refleja el nivel de impacto que puede tener la empresa si un incidente afecta a un activo, sin tener en cuenta las medidas de seguridad que existan sobre este.

|  |  |
| --- | --- |
| ACTIVOS | IMPACTO |
| Capa de negocio |  |
| * Información
 |  |
| * + Base datos de clientes
 | 10 |
| * + Base datos de empleados
 | 10 |
| * + Base datos productos
 | 8 |
| Servicios internos |  |
| * Ficheros de red
 | 7 |
| * Email
 | 8 |
| * Copias de seguridad
 | 9 |
| Equipamiento |  |
| * Software
 |  |
| * + Paquete office
 | 7 |
| * + Panda antivirus
 | 8 |
| * + AVG
 | 8 |
| * + Windows 7
 | 7 |
| * + Windows 8
 | 7 |
| * + Windows Server 2008 R2
 | 9 |
| * Hardware
 |  |
| Portatiles | 8 |
| PC’s | 8 |
| Servidores | 10 |
| Router | 9 |
| Multifunción | 6 |
| Fax | 6 |
| SAI | 7 |
| QNAP | 8 |
| Telefonía | 6 |

Factores de riesgo que pueden afectar a dichos activos, indicando la probabilidad de que esto suceda en una escala del 1 al 3.Se evalúa la probabilidad teniendo en cuenta las medidas existentes en la organización.

|  |  |
| --- | --- |
| FACTORES DE RIESGO | PROBABILIDAD |
| Abuso de puertos para mantenimiento remoto | 1 |
| Acceso no autorizado a datos (borrado, modificación,…) | 2 |
| Mal almacenamiento de passwords | 2 |
| Ancho banda insuficiente | 1 |
| Borrado, modificación o revelación desautorizada de información | 1 |
| Condiciones de trabajo adversas | 1 |
| Conexión cableado defectuosa | 1 |
| Conexiones activas | 3 |
| Mala configuración red | 2 |
| Copia no autorizada de un medio de datos | 2 |
| Destrucción negligente de datos | 2 |
| Denegación de servicio | 1 |
| Entrada sin autorización ha habitación | 2 |
| Formación usuarios inadecuada | 1 |
| Errores configuración y operación | 1 |
| Errores de software | 1 |
| Factores ambientales | 1 |
| Fallo base de datos | 1 |
| Fallo en WAN | 1 |
| Fallo medios externos | 1 |
| Falta de auditorias | 3 |
| Falta autenticación | 1 |
| Falta de confidencialidad | 1 |
| Falta cuidado manejo de la información | 2 |
| Falta de espacio de almacenamiento | 1 |
| Ingeniería social | 1 |
| Interferencias | 1 |
| Mal mantenimiento | 1 |
| Mal uso de derechos de administrador | 3 |
| Mal uso del servicio de mail | 2 |
| Mala administración de control de acceso | 1 |
| Mala configuración de fechas de backup | 1 |
| Mala evaluación de datos de auditoría | 3 |
| Mala integridad de los datos | 1 |
| Mantenimiento inadecuado | 2 |
| Datos no disponibles cuando son necesarios | 1 |
| Modificación no autorizado de datos | 1 |
| No cumplimiento medidas seguridad sistema | 2 |
| Penetración, intercepción o manipulación de líneas | 1 |
| Pérdida de backups | 2 |
| Perdida de confidencialidad en datos privados y de sistema | 1 |
| Pérdida de confidencialidad o integridad de datos por error humano | 2 |
| Pérdida de datos | 1 |
| Riesgo por personal externo | 1 |
| Robo | 1 |
| Robo de información | 1 |
| Robo de equipos portátiles | 1 |
| Sabotaje | 1 |
| Seguridad en base de datos deficiente | 1 |
| Software desactualizado | 1 |
| Spoofing y sniffing | 1 |
| Transferencia de datos incorrectos o no deseados | 1 |
| Transporte inseguro de archivos | 2 |
| Uso descontrolado de recursos (DoS) | 1 |
| Uso de derechos sin autorización | 1 |
| Virus, gusanos y troyanos | 3 |

 ***11.3 Posibles consecuencias***

(D-deficiente, M-mejorable, E-eficiente)

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Nombre del** |  | **Factor** |  | **de** | **¿Consecuencias?** |  | **¿Se** | **¿Cómo?** |  |  | **¿Es** |
| **archivo** |  |  | **riesgo** |  |  |  |  |  |  |  | **protege** |  |  |  |  | **efectiva?** |
|  |  |  |  |  |  |  |  |  |  |  | **?** |  |  |  |  |  |
| **Servidor y** |  | Acceso | no | Robo y | pérdida | de | Si | Acceso | físico | M |
| **router** |  |  | autorizado |  |  | información |  |  |  | restringido |  | y |  |
|  |  |  |  |  |  |  |  |  |  |  |  | seguridad lógica |  |  |
|  |  |  | Corte | de luz o | Perdida de integridad | si | Utilización de SAI | E |
|  |  |  | variaciones | de | y disponibilidad | de |  |  |  |  |  |  |
|  |  |  | voltaje |  |  |  | datos |  |  |  |  |  |  |  |  |  |
|  |  |  | Error |  | de | Aumento |  | de | si | Mantenimiento |  | M |
|  |  |  | configuración | vulnerabilidades | e |  | persona |  |  |  |
|  |  |  |  |  |  |  | inestabilidad | en | el |  | especializada |  |  |
|  |  |  |  |  |  |  | sistema |  |  |  |  |  |  |  |  |  |
|  |  |  | Factores |  |  | Interrupciones | en | el | si | Equipamiento actual | E |
|  |  |  | ambientales, |  |  | funcionamiento | del |  | y | mantenimiento |  |
|  |  |  | límite | de | vida | sistemas |  |  |  |  | especializado |  |  |
|  |  |  | útil, |  | Mal |  |  |  |  |  |  |  |  |  |  |
|  |  |  | mantenimiento |  |  |  |  |  |  |  |  |  |  |
|  |  |  | Modificación no | Inconsistencia |  | de | si | Acceso | físico | E |
|  |  |  | autorizada | de | datos, |  | mala |  | restringido |  | y |  |
|  |  |  | datos |  |  |  | configuración, fraude |  | seguridad lógica |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | Robo |  |  |  | Pérdida |  |  | de | Si | Controles | acceso | E |
|  |  |  |  |  |  |  | equipamiento |  | o |  | físico | y | lógico | al |  |
|  |  |  |  |  |  |  | información |  |  |  | servidor |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | Virus |  |  |  | Fallos | generales | en | Si | Herramientas |  | M |
|  |  |  |  |  |  |  | el sistema y en la red |  | antivirus y firewall |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Bases** | **de** |  | Copia |  | no | Divulgación | de | la | Si | Deshabilitación | del | E |
| **datos** |  |  | autorizada de un | información |  |  |  | portapapeles | y |  |
|  |  |  | medio de datos |  |  |  |  |  | controles lógicos |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  | Errores | de | Inconsistencia en los | Si | Controles internos y | M |
|  |  |  | software |  |  | datos |  |  |  |  | backup de los datos |  |
|  |  |  |  |  |  |  |  |
|  |  |  | Fallo en base de | Inconsistencia en los | Si | Controles internos y | E |
|  |  |  | datos |  |  |  | datos |  |  |  |  | backup de los datos |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  | Fallo en medios | Pérdida de backup |  | Si | Almacenamiento | en | E |
|  |  |  | externos |  |  |  |  |  |  |  | servidor externo |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Bases** | **de** | Falta de espacio | Fallo en la aplicación | Si | Disposición |  | de | E |
| **datos** |  | de |  |  |  |  |  | recursos |  |  | de |  |
|  |  | almacenamiento |  |  |  | almacenamiento | de |  |
|  |  |  |  |  |  |  |  | repuesto |  |  |  |  |
|  |  | Mala |  |  | Datos sin backup |  | Si | Revisar |  |  |  | E |
|  |  | configuración de |  |  |  | periódicamente | la |  |
|  |  | la | tabla | de |  |  |  | tabla |  |  |  |  |
|  |  | backups |  |  |  |  |  |  |  |  |  |
|  |  | Medios de datos | Pérdida de tiempo y | Si | Backup | disponible | E |
|  |  | no |  | están | productividad |  |  | inmediatamente |  |  |
|  |  | disponibles |  |  |  | para su utilización |  |  |
|  |  | cuando | son |  |  |  |  |  |  |  |  |
|  |  | necesarios |  |  |  |  |  |  |  |  |  |
|  |  | Pérdida | de | Incapacidad | de | Si | Backups |  |  |  | Si |
|  |  | backups |  | restauración |  |  | redundantes |  | en |  |
|  |  |  |  |  |  |  |  | posesión | de | la |  |
|  |  |  |  |  |  |  |  | empresa | y |  | en |  |
|  |  |  |  |  |  |  |  | servidores externos |  |
|  |  | Pérdida | de | Divulgación | de | Si | Controles | físicos | y | E |
|  |  | confidencialidad | información |  |  | controles | de | acceso |  |
|  |  | en |  | datos |  |  |  | lógicos | a | datos |  |
|  |  | privados | y de |  |  |  | críticos |  |  |  |  |
|  |  | sistema |  |  |  |  |  |  |  |  |  |
|  |  | Pérdida de datos | Inconsistencia | de | Si | Políticas |  |  | de | M |
|  |  | en tránsito |  | datos y divulgación |  | configuración de red |  |
|  |  |  |  |  | de información |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Nombre del** |  | **Factor** | **de** | **¿Consecuencias?** |  | **¿Se** | **¿Cómo?** |  |  | **¿Es** |
| **archivo** |  |  | **riesgo** |  |  |  |  | **protege** |  |  |  |  | **efectiva?** |
|  |  |  |  |  |  |  |  | **?** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| **Bases** | **de** |  | Portapapeles, |  |  | Divulgación | de | Si | Deshabilitación | de | E |
| **datos** |  |  | impresoras | o | información |  |  | portapapeles | y |  |
|  |  |  | directorios |  |  |  |  |  | controles lógicos |  |  |
|  |  |  | compartidos |  |  |  |  |  |  |  |  |  |  |
|  |  |  | Robo |  |  | Divulgación | de | Si | controles | lógicos | y | E |
|  |  |  |  |  |  | información |  |  | físicos |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | Robo por uso de | Divulgación | de | Si | Eliminar |  | la | E |
|  |  |  | equipos |  |  | información |  |  | información crítica |  |
|  |  | portátiles |  |  |  |  |  | de | los | equipos |  |
|  |  |  |  |  |  |  |  |  | portátiles |  |  |  |
|  |  |  | Sabotaje |  |  | Pérdida | o | Si | Backups |  |  | E |
|  |  |  |  |  |  | modificación | de |  | redundantes | y |  |
|  |  |  |  |  |  | datos, pérdida | de |  | controles | físicos | y |  |
|  |  |  |  |  |  | tiempo | y |  | lógicos |  |  |  |
|  |  |  |  |  |  | productividad |  |  |  |  |  |  |  |
|  |  |  | Spoofing | y | Divulgación | y | No |  |  |  |  | D |
|  |  |  | sniffing |  |  | modificación | de |  |  |  |  |  |  |
|  |  |  |  |  |  | información |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  | Transferencia de | Inconsistencia | de | Si | Controles lógicos |  | E |
|  |  |  | datos |  |  | datos |  |  |  |  |  |  |  |
|  |  |  | incorrectos |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | Virus |  |  | Pérdida, |  | Si | Herramientas |  | M |
|  |  |  |  |  |  | modificación | y |  | antivirus y firewall |  |
|  |  |  |  |  |  | divulgación de datos. |  |  |  |  |  |  |
|  |  |  |  |  |  | Perdida de tiempo y |  |  |  |  |  |  |
|  |  |  |  |  |  | productividad |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Nombre** | **del** | **Factor de riesgo** | **¿Consecuen** | **¿Se protege?** | **¿Cómo?** |  | **¿Es efectiva?** |
| **archivo** |  |  |  | **cias?** |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| **Software** | **de** | Aplicaciones | sin | Multas |  | y | si | Utilización |  | E |
| **aplicación** | **y** | licencia |  | problemas |  |  |  | de | software |  |
| **sistemas** |  |  |  | con software |  | libre | y |  |
| **operativos** |  |  |  | legal |  |  |  |  | compra | de |  |
|  |  |  |  |  |  |  |  |  | licencias |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | Error | de | Mal |  |  |  | Si | Utilización |  | E |
|  |  | configuración |  | funcionamie |  | de |  |  |  |
|  |  |  |  | nto | de | los |  | herramientas |  |
|  |  |  |  | sistemas |  |  |  | de | análisis | y |  |
|  |  |  |  |  |  |  |  |  | personal | de |  |
|  |  |  |  |  |  |  |  |  | mantenimien |  |
|  |  |  |  |  |  |  |  |  | to |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | Errores en | las | Problemas en | No |  |  |  | D |
|  |  | funciones | de | la |  |  |  |  |  |  |  |  |
|  |  | encriptación |  | recuperación |  |  |  |  |  |
|  |  |  |  | de | archivos |  |  |  |  |  |
|  |  |  |  | encriptados o |  |  |  |  |  |
|  |  |  |  | divulgación |  |  |  |  |  |  |
|  |  |  |  | de |  |  |  |  |  |  |  |  |
|  |  |  |  | información |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | Fallo del sistema | Falta |  | de | Si | Backup | y | M |
|  |  |  |  | sistema |  | y |  | sistemas | de |  |
|  |  |  |  | pérdida | de |  | respaldo |  |  |
|  |  |  |  | productivida |  |  |  |  |  |
|  |  |  |  | d |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  | Falta | de | Divulgación |  | Si | Desactivació | E |
|  |  | confidencialidad | de |  |  |  |  | n |  | de |  |
|  |  |  |  | información |  |  | portapapeles |  |
|  |  |  |  |  |  |  |  |  | y | controles |  |
|  |  |  |  |  |  |  |  |  | lógicos |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | Mala |  | Divulgación |  | Si | Controles | de | E |
|  |  | administración de | y |  |  |  |  | acceso |  |  |
|  |  | control de acceso | modificación |  | lógico, |  |  |
|  |  |  |  | de |  |  |  |  | reforzados en |  |
|  |  |  |  | información |  |  | datos críticos |  |
|  |  |  |  |  |  |  |  |  |
|  |  | Pérdida de datos | Divulgación |  | Si | Backup | de | E |
|  |  |  |  | de |  |  |  |  | respaldo |  |  |
|  |  |  |  | información |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  | Poca adaptación | Sistema |  |  | Si | Metodología | E |
|  |  | a cambios | del | inestable |  | y |  | de | análisis | y |  |
|  |  | sistema |  | de | difícil |  | diseño |  |  |
|  |  |  |  | modificación |  | estructurado |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Software | des- | Probabilidad | Si | Mantenimien | M |
|  | actualizado |  | incremental |  | to | por |  |
|  |  |  | de |  |  | especialistas |  |
|  |  |  | vulnerabilida |  | y constante |  |
|  |  |  | des y virus |  | evaluación |  |
|  |  |  |  |  |  | de |  |  |
|  |  |  |  |  |  | aplicaciones |  |
|  |  |  |  |  |  |  |
|  | Virus |  | Inestabilidad | Si | Herramientas | M |
|  |  |  | y | mal |  | antivirus | y |  |
|  |  |  | funcionamie |  | firewall |  |  |
|  |  |  | nto | del |  |  |  |  |
|  |  |  | sistema |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Nombre** | **del** | **Factor** | **de** | **¿Consecuen** | **¿Se protege?** | **¿Cómo?** | **¿Es efectiva?** |
|  | **archivo** |  |  | **riesgo** |  | **cias?** |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | **Backup** |  |  | Copia no |  | Robo de | Si | Controles de | M |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | autorizada a | información |  | acceso lógico |  |
|  |  |  |  | un medio de |  |  | al servidor |  |
|  |  |  |  | datos |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | Errores de |  | Error en la | Si | Backup en | E |
|  |  |  |  | software |  | generación o |  | medios |  |
|  |  |  |  |  |  | en la copia |  | externos en |  |
|  |  |  |  |  |  | de backups a |  | la empresa y |  |
|  |  |  |  |  |  | medios |  | en servidor |  |
|  |  |  |  |  |  | externos |  | externo |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | Falta de |  | Fallo en la | Si | Disco de alta | E |
|  |  |  |  | espacio de |  | generación |  | capacidad. |  |
|  |  |  |  | almacenamie | de backups |  | Disco |  |
|  |  |  |  | nto |  |  |  | redundante |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | Mala |  | Falta de | Si | Agenda de | E |
|  |  |  |  | configuració | copias de |  | backups |  |
|  |  |  |  | n de la tabla | seguridad |  | eficiente |  |
|  |  |  |  | de backups |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | Mala |  | Errores | Si | Varias copias | E |
|  |  |  |  | integridad de | durante la |  | de seguridad |  |
|  |  |  |  | los datos |  | restauración |  | en sitios |  |
|  |  |  |  | guardados |  | de datos |  | distintos |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  | Los datos no | Pérdida de | Si | Varias copias | E |
|  |  |  |  | están |  | backups y |  | de seguridad |  |
|  |  |  |  | disponibles | retraso del |  | en distintos |  |
|  |  |  |  | cuando son | sistema |  | lugares |  |
|  |  |  |  | necesarios |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Pérdida de | Falta de | Si | Backups | E |
|  | backups | datos, |  | redundantes |  |
|  |  | incapacidad |  |  |  |
|  |  | de |  |  |  |
|  |  | restaurarlos y |  |  |  |
|  |  | divulgación |  |  |  |
|  |  | de |  |  |  |
|  |  | información |  |  |  |
|  |  |  |  |  |  |
|  | Robo | Incapacidad | Si | Controles de | E |
|  |  | de |  | acceso |  |
|  |  | restaurarlos y |  | físicos, caja |  |
|  |  | divulgación |  | de seguridad, |  |
|  |  | de la |  | control de |  |
|  |  | información |  | acceso |  |
|  |  |  |  |  |  |
|  | Rotulación | Errores | Si | Rótulos | E |
|  | inadecuada | durante la |  | capaces de |  |
|  | en los | instalación |  | diferenciar |  |
|  | medios de | de datos |  | cada medio |  |
|  | datos |  |  | de datos |  |
|  |  |  |  | como único |  |
|  |  |  |  |  |  |
|  | Sabotaje | Pérdida o | Si | Controles de | E |
|  |  | robo de |  | acceso físico, |  |
|  |  | información |  | y copias de |  |
|  |  |  |  | respaldo |  |
|  |  |  |  | redundantes |  |
|  |  |  |  |  |  |
|  | Spoofing y | Divulgación | No |  | M |
|  | sniffing | , |  |  |  |
|  |  | modificación |  |  |  |
|  |  | y robo de |  |  |  |
|  |  | información |  |  |  |
|  |  |  |  |  |  |
|  | Virus | Pérdida de | Si | Herramientas | M |
|  |  | datos de |  | antivirus y |  |
|  |  | backup |  | firewall |  |
|  |  |  |  |  |  |

12 Plan de contingencias

 ***12.1 Administración de incidentes***

Se deberá asegurar la continuidad de la recolección de datos y su procesamiento ante cualquier contingencia que afecte a los centros de procesamiento. Para ello se deberá:

1. Generar **procedimientos manuales** de respaldo para cada una de las actividades desarrolladas en la empresa,
	1. Preparar, probar y mantener actualizado un **plan de contingencias**, coordinando el mismo con los procedimientos de copias de respaldo y almacenamiento externo. Dicho plan deberá ser desarrollado de forma que cubra las distintas áreas de riesgo,
	2. Definir y asignar claramente las **responsabilidades** de las tareas detalladas en el plan,
	3. Prever un programa de **entrenamiento** para el personal involucrado en el plan de contingencias.
* Deberá almacenarse una **copia del plan** de contingencias en el exterior de la empresa, protegiéndola contra su divulgación y actualizándola permanentemente.

***12.2 Backup de equipamiento***

• El equipamiento informático de la empresa debe contar con **dispositivos de** **respaldo**, ante cualquier tipo de incidente.

Debe haber un ordenador portátil de respaldo con las mismas aplicaciones que el ordenador principal, con acceso al Server y a toda la información, debe estar a punto para poder ser utilizado en cualquier momento.

La organización también dispondrá de un servidor de backup correctamente configurado para su inmediato funcionamiento.

Se dispondrá de un router de repuesto por posibles incidentes en este.

Se dispondrá de otro disco duro externo de la misma capacidad (1’5 TB) donde se volcara la información si el disco duro principal fallará.

La información se volcaría desde el servidor.

Un equipo de fax de respaldo, para substituirlo por el principal en el caso de que este fallará.

* Los **mecanismos de recuperación** de los dispositivos de respaldo deben ser probados periódicamente comprobando su buen funcionamiento.
* El sistema informático no deberá verse afectado ante una contingencia en el centro de trabajo, por lo que el equipamiento informático debe distribuirse en **lugares físicos diferentes**, contando ambos con las medidas y condiciones decalidad y seguridad especificadas en esta política, distribuyendo de esta manera el equipamiento redundante.

El equipamiento informático de backup estará ubicado en el despacho del abogado donde recibe a las visitas, más o menos a unos 800 m de su lugar de trabajo.

Así la reposición de cualquier equipo será rápida y eficaz.

• En el caso que ocurra alguna **contingencia con el servidor** de aplicaciones, se utilizará un servidor de backup configurado exactamente igual que el servidor principal, los datos que se encuentran en el servidor principal se volcaran al servidor de backup gracias al disco duro externo.

 ***12.3 Plan de recuperación***

* Debe conformarse un **grupo de desarrollo** encargado de concebir, probar e implementar el plan de contingencias. Éste debe estar a cargo del administrador de la organización y supervisado por el gerente de esta.
* Debe asignarse un **orden de importancia** a los sistemas de información y a los equipos de la red informática, de acuerdo al análisis de riesgo y al impacto que representaría para la empresa su ausencia.

Dicho orden sería el siguiente:

-instalar el servidor de backup con las aplicaciones necesarias -Realizar la conexión a la red

-Recuperar los datos guardados en el disco externo y volcarlos al servidor de backup.

-Poner en marcha el equipo portátil de backup correctamente configurado.

* Los equipos deberán estar **señalizados** o etiquetados de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.
* Deberán definirse las funciones o **servicios críticos** de la empresa, junto con los recursos mínimos necesarios para su funcionamiento, asignándoles una prioridad en el plan de contingencia.

Los recursos mínimos de nuestra organización serán:

-Servidor con las aplicaciones necesarias, en su defecto, PC, con dichas aplicaciones listo para ser utilizado.

-Datos que maneja la organización ya antes citados.

-PC o portátil de backup para la realización de las tareas.

-Conexión a Internet.

* Deberán identificarse las **contingencias** que podrían ocurrir para cada nivel de servicio crítico definido.
* Deberá conformarse un **plan de emergencias**, determinando los procedimientos a llevar a cabo para cada contingencia identificada, considerando los distintos escenarios posibles. Cada procedimiento deberá estar claramente definido, y tener asignado un responsable para su ejecución.
* Para el desarrollo del plan de contingencias deben contemplarse las siguientes pautas:
	1. Deberá estar **documentado** y **testeado** antes de su puesta en práctica.
	2. Deberá basarse en un **análisis de riesgo**, determinando que acciones merecen estar incluidas.
	3. Deberá **abarcar** la totalidad de la empresa.
	4. Deberá mantenerse **actualizado** de acuerdo a nuevos puestos de trabajos y funciones.
	5. Deberá ser **probado** frecuentemente.
	6. Deberá **contener** la siguiente información:
		+ objetivo del plan,
		+ modo de ejecución,
		+ tiempo de duración,
		+ costes estimados,
		+ recursos necesarios,
		+ evento a partir del cual se pondrá en marcha el plan
	7. Debe definirse hasta cuanto tiempo se aceptará estar en **condición de** **emergencia**.
	8. • Debe documentarse la realización de las siguientes actividades **después** **de un incidente**:
* determinar la causa del daño,
* evaluar la magnitud del daño que se ha producido,
* que sistemas se han afectado,
* qué modificaciones de emergencia se han realizado,
* que equipos han quedado no operativos,
* cuales se pueden recuperar y en cuanto tiempo.

13 App

Para el desempeño eficiente de la auditoria he decidido realizar una aplicación móvil.

En ella se pondrá realizar la auditoria mediante el dispositivo móvil, ser almacenada y compartida al instante.

Actualmente existe una versión en pruebas para Android completamente funcional.

Ver ANEXO 2.

14 Conclusiones

Una vez finalizada la auditoría he llegado a la conclusión de que las ISO son de vital importancia ya no tanto en grandes empresas sino en medianas empresas para volverla mucho más competitivas y conseguir un espacio en el sector de las grandes empresas donde la eficiencia y eficacia se convierten en un requisito indispensable.

Concretando en la ISO 27001, muestra unas pautas de control para garantizar la seguridad en la información y que el conjunto de estos recursos estén destinados a lograr que la empresa y los activos de esta sean confidenciales, íntegros y disponibles para todos los usuarios.

Están proliferando continuamente los ataques para la extracción de información por el valor que posee en el mercado por eso es sumamente difícil cubrir por completo todos los riesgos y amenazas que existen pero siempre se debe tener una postura proactiva, intentar adelantarse a los acontecimientos intentando abastar el máximo posible. De ahí la importancia de implantar unas políticas y buenas maneras de uso de seguridad de información.

Una vez terminado el proyecto puedo concluir que los resultados han sido muy satisfactorios para ambas partes, me ha servido para conocer un gran sector como es el de las auditorias, que actualmente se encuentran en aumento dentro del marco europeo, a su vez me ha aportados amplios conocimientos sobre cómo se debe gestionar un SGSI y la gran importancia y utilidad de este.

Por otro lado el análisis realizado a la empresa ha sido de gran ayuda para el director de sistemas de información de la empresa puesto que le ha dado aspectos a mejorar en la seguridad de la información acompañado de las pautas correctas a seguir para obtener la certificación de la ISO 27001 deseada.

15 Bibliografía

1. *Portal de la ISO 27001 en español http://www.iso27000.es/*
2. *entorno de análisis de riesgos http://www.ar-tools.com/*
3. *Sistemas de gestión de seguridad de la información http://sgsi-iso27001.blogspot.com/*
4. Enciclopedia libre Wikipedia *ISO/IEC 27001*
5. Enciclopedia libre Wikipedia *LOPD*
6. *Seguridad informática http://www.rzw.com.ar/seguridad-informatica-4409.html*
7. *Libro electrónico seguridad informática y criptografía http://www.criptored.upm.es/guiateoria/gt\_m001a.htm*
8. *Libro: Auditoría informática, un enfoque práctico.*