DISEÑAR LOS CONTROLES DE ACCESO APLICABLES A LA EMPRESA SPYTECH S.A.S PARA SU POSTERIOR IMPLEMENTACIÓN, DE ACUERDO CON EL DOMINIO A9 DE LA NORMA ISO 27001:2013

MARILUZ GARZÓN GARZÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, CUNDINAMARCA
2017

DISEÑAR LOS CONTROLES DE ACCESO APLICABLES A LA EMPRESA SPYTECH S.A.S PARA SU POSTERIOR IMPLEMENTACIÓN, DE ACUERDO CON EL DOMINIO A9 DE LA NORMA ISO 27001:2013

MARILUZ GARZÓN GARZÓN

Tesis de grado para optar por el título:

Especialista en Seguridad Informática

Director de Proyecto:

Ing. Martin Camilo Cancelado Ruiz

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ, CUNDINAMARCA

2016

Nota de Aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, 30 de Marzo de 2017.

1. DEDICATORIA

Dedico este trabajo a Dios, a mi tía Hilda María Garzón y a mis padres; ellos fueron el motivo para seguir adelante. A mis profesores, quienes nunca desistieron al enseñarme, aun sin importar que muchos no valoramos sus esfuerzos. A mis amigos, quienes siempre estuvieron dando fuerza moral para continuar, cuando quería desistir de seguir con mis metas.

2. AGRADECIMIENTOS

Agradezco a todos mis profesores, quienes durante un largo perdido estuvieron ahí, dispuestos a dar lo mejor de sí sin importar qué tan duro fuera. Ellos fueron mis mentores, siempre dispuestos a buscar la excelencia en mi profesión.

Hoy solo puedo decirles gracias por todas sus enseñanzas, consejos y dedicación.

CONTENIDO

Pag.

LISTA DE TABLAS

Pag.

3. LISTA DE FIGURAS

4. LISTA DE ANEXOS

ANEXO A. Bioscrypt4GSTS-DataSheet
ANEXO B. Nombre
ANEXO C. Nombre

GLOSARIO

ACCIÓN CORRECTIVA: Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

ACTIVO: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

ALCANCE: Ámbito de la organización que queda sometido al SGSI.

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

CONTROL: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información, por debajo del nivel de riesgo asumido. Control, es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

ISO/IEC 27001: Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

ISO/IEC 27002: Código de buenas prácticas en gestión de la seguridad de la información. Primera publicación en 2005; segunda edición en 2013. No es certificable.

VULNERABILIDAD: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

SEGURIDAD DE LA INFORMACIÓN: Proceso continuo para salvaguardar la confidencialidad, integridad y disponibilidad de la información.

5. INTRODUCCIÓN

Desde hace ya algunos años la información se considera uno de los activos más valiosos de una compañía (los costos derivados de la perdida de la información no sólo son costos económicos directos, sino que también afectan a la imagen de la empresa). Cada vez más la seguridad de la información forma parte de los objetivos de las organizaciones; sin embargo, a pesar de la concienciación generalizada, muchas compañías no se enfrentan a este aspecto con la seriedad que debiera tratarse.

La continua evolución, crecimiento y sofisticación de la tecnología, al igual que los ataques cibernéticos en las organizaciones, ponen de manifiesto la necesidad de adoptar las medidas y controles que permitan proteger a la compañía ante las amenazas a los activos de información. De esta manera se hace necesario diseñar un sistema de información que permita salvaguardar los recursos informáticos de SPYTECH S.A.S.

Con el fin de mitigar

6. PLANTEAMIENTO DEL PROBLEMA

Actualmente la empresa SPYTECH S.A.S se establece en el mercado como una organización privada, dedicada a la prestación de servicios de seguridad informática. Su origen es finlandés y cuenta con más de 25 años de experiencia en el ámbito mundial. En Colombia se estableció en 2011 y presta sus servicios a los sectores educativo, privado y gubernamental, por lo que la información a la que tiene acceso la entidad requiere del establecimiento de mecanismos de protección con el fin de garantizar su confidencialidad.

SPYTECH S.A.S actualmente no cuenta con los mecanismos necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información; por lo cual el personal interno y externo puede tener acceso a la misma, con el riesgo de dejar los datos expuestos a alteraciones, degradación o pérdida total. , con el fin de mitigar se debe plantear mecanismos, políticas y procedimientos que permitan controlar el acceso a la información desde cualquier medio (USB, Wiffi, SD, Dispositivos Móviles, Laptops, Conexiones Remotas).

¿Cómo se pueden mejorar los niveles de acceso a la empresa SPYTECH S.A.S, y dar cumplimiento a lineamientos de seguridad de la información?

7. JUSTIFICACIÓN

Los incidentes de seguridad de Tecnologías de la Información (TI) representan una grave amenaza para la ejecución eficiente de las estrategias corporativas. Lo que se busca es que la organización SPYTECH S.A.S establezca controles de acceso lógicos basados en la norma ISO 27001:2013 para el personal interno o externo, con la respectiva definición de políticas y procedimientos que determinen los lineamientos necesarios, con el fin de que los procesos se ejecuten de acuerdo con un protocolo específico que garantice la integridad y la confidencialidad de la información.

El Sistema de Gestión de Seguridad de la Información – en adelante, SGSI- permite identificar, gestionar y minimizar los riesgos reales y potenciales de la seguridad de la información de una organización, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y en las tecnologías.

Por ello, debido a la criticidad de la información a la que tiene acceso SPYTECH S.A.S, proveniente de sus clientes, se hace necesario establecer mecanismos que

permitan mantener la confidencialidad de la misma, dentro y fuera de la organización.

8. OBJETIVOS

8.1. OBJETIVO GENERAL

Sugerir los controles de acceso para minimizar los riesgos de seguridad de la información, con el cumplimiento de la confidencialidad, integridad y disponibilidad que define la norma ISO 27001:2013.

8.2. OBJETIVOS ESPECÍFICOS

- Realizar un análisis del estado actual de los controles de acceso de acuerdo con el dominio A.9 del anexo A de la norma ISO 27001:2013, y recomendar los controles aplicables así como mejoras a los controles existentes.
- Diseñar una política de control de acceso para SPYTECH S.A.S, de conformidad con la Norma ISO 27001:2013.
- Garantizar el acceso a sistemas de información y servicios a los usuarios autorizados, e impedirlo a los no autorizados.

9. MARCO REFERENCIAL

Actualmente la información es el activo más valioso de una organización, por lo que se hace necesario establecer mecanismos para protegerla, con el objetivo de evitar la pérdida parcial o total de la misma, lo que puede llevar a las organizaciones a sufrir consecuencias catastróficas.

Los avances en la tecnología y el uso de las mismas han experimentado un crecimiento importante en los últimos años y con ello crecen los riegos de sufrir un incidente de seguridad de la información, en la mayoría de las ocasiones los ataques son realizados con fines criminales, sabotaje o en ocasiones con el fin de determinar que tanto se puede acceder a la información de una organización, estos ataques pueden llegar a generar costos y pérdidas para la organización y en ocasiones el cierre de la organización .

Para gestionar la seguridad de la información hay que involucrar a toda la organización y sus miembros, la dirección y en ocasiones los proveedores, con el fin de definir la política en la cual se establecerán las directrices a seguir.

Mediante un sistema de gestión de Seguridad de la Información (SGSI), la organización conoce los riesgos a los que su información se ve expuesta, manteniéndolos en un nivel mínimo, implementando controles, documentado cada uno de los procesos.

10. MARCO CONCEPTUAL

A continuación, se presentan algunas definiciones relacionadas al SGSI que se busca implementar.

- Información: Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. La información, ya sea impresa, almacenada digitalmente o hablada. Actualmente es considerada como un activo dentro de las compañías y que se debe proteger, ya que es de gran importancia.[ISO/IEC 27000]
- Riesgo: Se define como cualquier impedimento, obstáculo, amenaza o problema que pueda impedirle a la empresa que alcance un objetivo. Se puede ver también como la posibilidad de sufrir un daño o pérdida. Se mide en términos de impacto y probabilidad de ocurrencia. [ISO/IEC 27000]
- Políticas de seguridad**:** Busca establecer reglas para proporcionar la dirección gerencial y el soporte para la seguridad de la información. Es la base del SGSI. [ISO/IEC 27000]
- Control de accesos**:** Los medios para asegurar que el acceso a los activos está autorizado y restringido, basado en los negocios y la seguridad requisitos. [ISO/IEC 27000]
- Seguridad de la información: Es la preservación de la confidencialidad, integridad y disponibilidad de la información. Además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas. [ISO/IEC 27000]
- Confidencialidad: Propiedad de que la información no esté disponible, es decir, revelada a personas, entidades, o procesos no autorizados

- Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. [ISO/IEC 27000]
- Disponibilidad: Propiedad de ser accesible y utilizable por petición de una entidad autorizada. [ISO/IEC 27000]
- Ataque: Intento de destruir, exponer, alterar, inutilizar, robar u obtener acceso no autorizado, o hacer un uso ilegítimo o indebido de un activo. [ISO/IEC 27000]
- Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva para determinar el grado en que se cumplen los criterios que sean definidos. [ISO/IEC 27000]
- Autenticación: Prestación de la garantía de que una característica alegada de una entidad es correcta. [ISO/IEC 27000]
- Mejora continua: Actividad recurrente para mejorar el rendimiento.
- Control: Medida que modifica un riesgo. [ISO/IEC 27000]

11. MARCO TEÓRICO

La ISO/IEC 27001:2013 es una norma internacional, emitida por la Organización Internacional de Normalización ISO (International Organization for Standardization). Indica qué requisitos deben conformar un SGSI y describe cómo gestionar la seguridad de la información en una empresa. La ISO/IEC 27001:2013 es actualmente el único estándar aceptado internacionalmente para la administración de la seguridad de la información y aplica a todo tipo de organización, tanto por su tamaño como por su actividad.

El estándar fue diseñado para promover un modelo que le permita a las organizaciones una reducción y eliminación importante de incidentes de seguridad, y al estar dentro del ciclo de mejora continua, hacer que el sistema de gestión responda a las nuevas necesidades de seguridad que vayan apareciendo dentro de la organización.

11.1. ESTRUCTURA DE LA ISO 27001:2013

El principal objetivo de la norma ISO 27001:2013 es proteger la confidencialidad, integridad y disponibilidad de la información en una organización. Actualmente esta norma contiene 144 controles de seguridad, 14 dominios y 130 requisitos de gestión.

Figura 1. Comparativo entre versiones de norma ISO 27001

ISO/IEC 27001: 2005	ISO/IEC 27001: 2013	
- **Nº CONTROLES**		
133 →	**114**	Se mantienen 94 y se eliminan 39. 20 son nuevos.
+ DOMINIOS DE SEGURIDAD		
11 →	**14**	
+ REQUISITOS DE GESTIÓN		
102 →	**130**	

Fuente: International Organization for Standardization

La gestión de la seguridad de la información (SGSI) no solo está enfocada a las tecnologías de la información (TI), sino también a trabajar de una forma global los procesos de una organización, (recurso Humano, Protección física).

11.2. IMPORTANCIA DE LA ISO 27001 DENTRO DE UNA ORGANIZACIÓN

El diseño e implementación de SGSI de una organización están determinados por las necesidades y los objetivos de la organización, así como por los requisitos de seguridad, los procesos de negocio, los empleados y el tamaño y la estructura de la organización. El diseño y la operación de un SGSI tienen que reflejar los intereses y la información, y los requisitos de seguridad de todas las partes interesadas de la organización, incluidos los clientes, proveedores, socios de negocios, accionistas y otros terceros relevantes.

Se espera que la adopción de un SGSI en una organización se integre perfectamente a las necesidades de la organización, así mismo debe de ser escalable y se y se actualice de acuerdo con los cambios que surjan dentro de la organización.

11.3. BENEFICIOS DE UN SGSI

El beneficio de la implementación de un SGSI es principalmente la reducción de los riesgos de seguridad de la información (es decir, reducir la probabilidad y /o el impacto causado por los incidentes seguridad de la información).

Otros beneficios que se obtienen, a partir de la adopción de la familia de normas del SGSI, son:

11.3.1. Cumplir con los requerimientos legales. El aumento en las normas y requerimientos, relacionados con la seguridad de la información, hace que las organizaciones busquen mecanismos de cumplimiento. En la mayoría de los casos todas estas normas y requerimientos son solucionados con la implementación de la norma ISO 27001:2013.

11.3.2. Obtener una ventaja comercial. Si una organización está certificada en ISO 27001 genera un nivel de confianza más alto entre sus clientes, frente a los que no la tienen.

11.3.3. Menores costos. Como el principal objetivo de la norma busca evitar incidentes de seguridad de la información que le puedan generar costos adicionales a la organización, se ahorra dinero en la atención de esas posibles eventualidades.

11.3.4. Una mejor organización. El rápido crecimiento las múltiples actividades no les permite a las organizaciones tener procesos bien definidos; por lo que la implementación de la ISO 2700:2013 les ayudará a definir este tipo de situaciones, a partir de procedimientos claros.

11.4. ÁREAS EN LAS QUE INTERVIENE LA SEGURIDAD DE LA INFORMACIÓN

La ISO 27001 interviene en el ámbito global de la organización a través de la interacción con procesos específicos (véase figura 2).

Figura 2. Procesos que interactúan en la seguridad de información

Fuente: http://www.newvisionsoftlan.com/img/riesgo.png

11.5. SECCIONES DE LA NORMA

ISO/IEC 27001 se divide en 11 secciones, más el anexo A, la norma específica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información, en la cual se especifican los requisitos

para la aplicación de los controles de seguridad de la información a medida de las necesidades de organizaciones o parte de las mismas.

Desde su publicación en 2005, la norma ISO 270001 no había sufrido ninguna modificación; sino hasta el año 2013 cuando fue revisada y aprobada la nueva versión (ISO/IEC 27001:2013).

Sus principales cambios se relacionan con la estructura de la parte principal de la norma, partes interesadas, objetivos, el monitoreo y la dedicación. El anexo A disminuyó los controles de 133 a 114, pero en cambio, incrementó las secciones de 11 a 14. También, se eliminaron algunos requerimientos como las medidas preventivas y la necesidad el documentar determinados procedimientos.

12. MARCO LEGAL

Para el diseño de un sistema de seguridad de la información se debe de cumplir con las leyes, normas, decretos, que sean aplicables en el desarrollo de las actividades.

12.1. DERECHOS DE AUTOR

- Decisión 351 de la C.A.N.
- Decreto 1360 de 1989
- Ley 565 de 2000

12.2. DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS

- Ley 1273

12.3. COMERCIO ELECTRÓNICO Y FIRMAS DIGITALES

- Ley 527 de 1999
- Decreto 1747 de 2000
- Resolución 26930 de 2000

12.4. LEY 34/2002 DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO (LSSI).

Esta Ley se encarga de regular las obligaciones de los prestadores de servicios y los servicios que prestan.

12.5. LEY 32/2003, GENERAL DE TELECOMUNICACIONES

El objeto de esta Ley es la regulación de las telecomunicaciones. Entre los objetivos están:

- Fomentar la competencia.
- Garantizar el cumplimiento de las obligaciones de servicio público en la explotación de redes y la prestación de servicios de comunicaciones electrónicas.
- Promover el desarrollo del sector de las telecomunicaciones.
- Hacer posible el uso eficaz de los recursos limitados de telecomunicaciones.
- Defender los intereses de los usuarios.

- Fomentar, en la medida de lo posible, la neutralidad tecnológica en la regulación.
- Promover el desarrollo de la industria de productos y servicios de telecomunicaciones.
- Contribuir al desarrollo del mercado interior de servicios de comunicaciones electrónicas en la Unión Europea.

12.6. LEY 59/2003 DE FIRMA ELECTRÓNICA

Esta Ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

12.7. LEY 1341 DEL 30 DE JULIO DE 2009

Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC- Se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

12.8. LEY 1273 del 2009

Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado-denominado “De la Protección de la Información y de los datos” y se preservan íntegramente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

13. DECLARACIÓN DE APLICABILIDAD

La declaración de aplicabilidad es una relación de los objetivos y controles que la organización seleccionó como adecuados a sus necesidades de negocio. También, registrará exclusiones de cualquier control. En definitiva, es un documento que demuestra cómo la organización controla los riesgos, pero no debe ser lo suficientemente detallado como para dar información valiosa que pudiese estar en manos de aquellos quienes puedan hacer mal uso de ella.

Figura 3. Ejemplo de una declaración de aplicabilidad

Cláusula N°	Objetivos de Control	Control	Aplica SI/NO	Documento Relacionado o Justificación
A.5	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**			
	A.5.1 Orientación de la dirección de la Seguridad de la Información	A.5.1.1 Políticas de seguridad de la información		
		A.5.1.2 Revisión de las políticas de seguridad de la información		
A.6	**ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN**			
	A.6.1 Organización Interna	A.6.1.1 Funciones y responsabilidades de la seguridad de la información		
		A.6.1.2 Separación de funciones		
		A.6.1.3 Contacto con autoridades		
		A.6.1.4 Contacto con grupos de interés especial		
		A.6.1.5 Seguridad de información en gestión de proyectos		
	A.6.2 Dispositivos Móviles y Teletrabajo	A.6.2.1		
		A.6.2.2		
A.7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**			

Cláusula N°	Objetivos de Control	Control	Aplica SI/NO	Documento Relacionado o Justificación
	A.7.1 Previo al Empleo	A.7.1.1		

Fuente: Autor

13.1. CONTROL DE ACCESO A LA INFORMACIÓN

Los controles bajo la norma ISO 2700:2013 se basan sobre políticas, procedimientos e implementación técnica. Se encargan de determinar las reglas necesarias para prevenir las vulnerabilidades de seguridad de la información, y limitar el acceso a la información y a los recursos de personal no autorizado. Estos controles deben establecer aplicación, seguimiento, revisión y mejora, cuando sea necesario, para asegurar el cumplimiento de los objetivos específicos de la seguridad y de negocio de la organización.

La selección de los controles depende de decisiones de la organización sobre la base de los criterios de aceptación del riesgo, las opciones de tratamiento del riesgo y el enfoque general de gestión de riesgos aplicado a la organización.

13.2. OBJETIVO DE CONTROL, SEGÚN NORMA ISO 27001

Según la norma, el acceso a la información, a los servicios de procesamiento de información y a los procesos del negocio, se deberán controlar según requisitos de seguridad y del negocio. Las reglas para el control del acceso deberían tener en cuenta las políticas de distribución y autorización de la información.

A continuación, se presenta un ejemplo de objetivos de control.

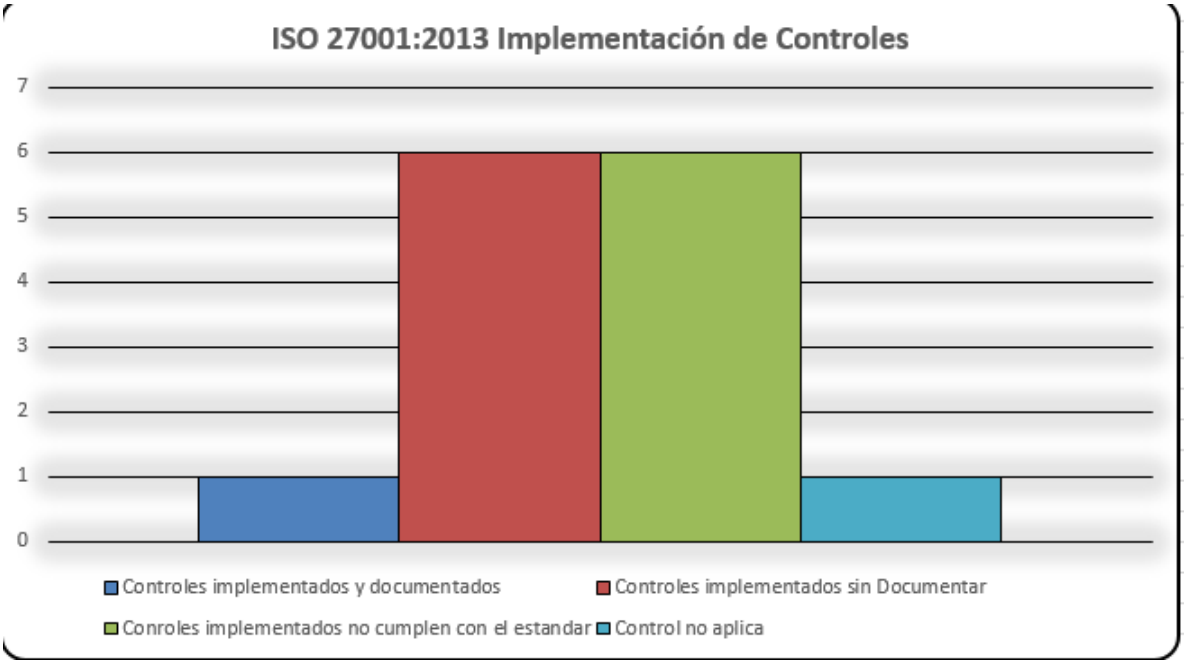
Tabla 1. Ejemplo de controles de información

Amenaza	Vulnerabilidad	Controles sugeridos en el ISO 27001 de control de acceso
Acceso no autorizado a información por exceso de privilegios	• No existe una política de control de acceso • No existen roles • Se tienen usuarios desactualizados	• A.9.1.1 Política de control de • acceso • A.9.2.3 Gestión de derechos de acceso privilegiado.
Acceso no autorizado a información por selección de contraseña o administración de contraseña	• Uso de contraseñas simples. • Falta de responsabilidad de usuarios • Contraseñas que no expiran	• A.9.4.3Sistema de Gestión de Contraseñas
Acceso no autorizado a la información por falta de una identificación y autorización única	• Proceso de verificación de identidad para cambio de contraseña. • Aplicaciones con su propio repositorio de identidad	• A.9.2.1 Registro y cancelación de registros usuarios • A.9.2.4 Gestión de Información de autenticación secreta de usuarios.
Acceso no autorizado a las aplicaciones de la compañía	• Alteración del contenido de la información. • Ruido de información	• A.9.4.1 Restricción de acceso a la información. • A.9.4.4 Uso de programas utilitarios privilegiados. • A.9.4.5 Control de Acceso a códigos fuente de programas.

Fuente: Elaboración Propia

Estado inicial de los controles en Spytech

En la siguiente grafica se evidencia que actualmente Spytech cuenta con diferentes controles que no están documentados, otros que están implementados pero que no cumplen con el estándar según la norma ISO 27001:2013, motivo por el cual deben ser rediseñados.



Fuente: Elaboración Propia

14. DISEÑO METODOLÓGICO PRELIMINAR

La metodología que se implementará en el proyecto es de tipo cualitativo descriptivo. Los estudios descriptivos, buscan especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis.

14.1. INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Se realizarán entrevistas de preguntas abiertas, con el fin de dar respuesta a la pregunta de investigación e indagar si se cumplieron los objetivos en la implementación del proyecto. También se realizará un cuestionario con preguntas abiertas con el fin de analizar y evaluar el estado actual de los controles de acceso de la compañía SPYTECH S.A.S. Se buscará, después de aplicar los dos instrumentos de recolección de datos anteriormente mencionados, realizar la triangulación de los mismos y el respectivo análisis cualitativo.

14.2. RECURSOS DISPONIBLES

Para la elaboración del proyecto se contará con los recursos humanos y profesionales capacitados en el manejo e implementación de la norma ISO 27001. Asimismo, se contará con los recursos tecnológicos, como computadores y software.

15. PRESUPUESTO

Tabla 2. Presupuesto del proyecto

Cantidad	Descripción	Valor mensual	Duración	Valor total
01	Gerente general líder del proyecto	4000000	6 meses	24.000.000,00
01	Ingenieros de sistemas especialistas en ISO 27001	3000000	6 meses	18.000.000,00
01	Ingenieros de sistemas o electrónicos	2000000	6 meses	12.000.000,00
01	Secretaria	800000	6 meses	4.800.000,00
01	Arrendamiento de oficina	1000000	6 meses	6.000.000,00
	Servicios públicos	1000000	6 meses	6.000.000,00
	Arrendamiento de computadores	1500000	6 meses	9.000.000,00
	Capacitación	6000000	1 mes	6.000.000,00
TOTAL				85.800.000,00

Fuente: Elaboración Propia

16. CRONOGRAMA

Figura 4. Cronograma del proyecto

Cronograma de Actividades	**Bimestre 1**	**Bimestre 2**	**Bimestre 3**	**Bimestre 4**
Diseño de Política de control de acceso				
Diseño de registro y cancelación del registro de usuarios				
Diseño de la gestión de derechos de acceso privilegiado				
Implementación de la gestión de información de autenticación secreta de usuarios				
Revisión de los derechos de acceso de usuarios				
Retiro y ajuste de los derechos de acceso a la información				
Auditorías				

Fuente: Elaboración Propia

17. DESARROLLO DEL PROYECTO

La implementación de los controles de acceso necesarios, que garanticen la seguridad de la información dentro de las instalaciones de SPYTECH S.A.S permitirá establecer mecanismos de supervisión para todo el personal que ingresa a las instalación de la organización.

El proyecto se realizará en varias etapas, con el fin de establecer progresivamente los parámetros y mecanismos que lleven a la realización y cumplimiento de los diferentes objetivos planteados.

17.1. PRIMERA ETAPA

En esta primera etapa se analizará y evaluará el nivel de seguridad actual con el que cuenta la compañía SPYTECH S.A.S.

Tabla 3. Evaluación del nivel de seguridad

Número	Vulnerabilidad	Existe
1	Control de ingreso y salida de personas a la instalaciones	NO
2	Control de ingreso y salida de elementos tecnológicos	NO
3	Aseguramiento físico de equipos de cómputo (portátiles)	NO
4	Aseguramiento físico de discos duros, discos extraíbles, y USB que contienen información sensible para la compañía.	NO
5	Aplicación de cláusulas de confidencialidad de la información a empleados que manejan datos sensibles para la compañía.	NO
6	Políticas de backup	NO
7	Definición de perfiles y roles	NO
8	Políticas de transferencia de conocimiento	NO

Fuente: Elaboración Propia

17.1.1. Control de ingreso y salida de personas a las instalaciones de la compañía SPYTECH S.A.S. Es necesario que la compañía pueda identificar, conocer y establecer un nivel de control al personal que ingresa a sus instalaciones. En la actualidad el ingreso se realiza de forma tradicional; Los visitantes se anuncian en la recepción y siguen hacia la oficina anunciada. Los empleados, por su parte (directivos, operadores, secretarias, etc.), tienen acceso total a todas las áreas de la compañía, sin ningún tipo de control.

17.1.2. Control de ingreso y salida de elementos tecnológicos. Los elementos tecnológicos son activos muy valiosos para la compañía, y es fundamental poder controlar y conocer cuáles activos están bajo riesgo al salir de la misma, cuáles elementos ingresan a las instalaciones y con qué motivo o fin ingresa un elemento a las instalaciones.

17.1.3. Aseguramiento físico de equipos de cómputo (portátiles). En la actualidad no se cuenta con políticas de aseguramiento y responsabilidad personal de elementos físicos; de tal manera que estos se puedan hurtar de la oficina sin dificultad.

17.1.4. Aseguramiento físico de discos duros, discos extraíbles y USB que contienen información sensible para la compañía. No existen en la compañía políticas que exijan o determinen cuáles son los discos externos que contienen información de carácter privado, ni se tiene claro bajo quién debe estar la custodia de estos elementos, ni el sitio donde deben residir dichos dispositivos.

17.1.5. Aplicación de cláusulas de confidencialidad de la información a empleados que manejan datos sensibles para la compañía. Es imperioso proteger la información de la compañía e informar a los trabajadores las pautas y tratamiento de la información confidencial y sus límites establecidos, con el fin de evitar malas

prácticas como, por ejemplo, llevarse las bases de datos o información sobre nuevos productos y sus desarrollos.

17.1.6. Políticas de Backups. Las buenas prácticas, que con el tiempo se convierten en hábitos, permiten a la compañía mantener resguardada y disponible información que, por diferentes motivos, pueda ser modificacada o destruida. Es necesario que se diseñe una política de backups, con el fin de garantizar la disponibilidad de la información.

17.1.7. Definición de perfiles y roles. Es necesaria la definición de los roles y perfiles en la empresa, con el objeto de autorizar y controlar los recursos de la compañía, sobre la base de la misión y función de los empleados.

17.1.8. Políticas de transferencia de conocimiento. Para mantener la continuidad del negocio es muy importante y necesario trasferir conocimiento y establecer reglas y procedimientos que resuelvan eventualidades.

18. EL CONTROL DE ACCESO

18.1. Los requerimientos del negocio de control de acceso

Objetivo: limitar el acceso a las instalaciones de procesamiento de la información y de la información.

18.1.1. Política de Control de Acceso

Una política de control de acceso debe ser establecida, documentado y revisado sobre la base de los negocios y requisitos de seguridad de la información.

Los propietarios de activos deben determinar las reglas de control de acceso apropiadas, derechos de acceso y restricciones para roles de usuario específicas para con sus activos, con el nivel de detalle y el rigor de los controles reflejando los riesgos de seguridad de la información asociada.

Los controles de acceso son a la vez lógica y física y estos deben ser considerados en conjunto. Los usuarios y los proveedores de servicios deben tener una declaración clara de los requerimientos del negocio que deben cumplir por los controles de acceso.

La política debe tener en cuenta lo siguiente:

a) Los requisitos de seguridad de las aplicaciones de negocio;
b) Las políticas para la difusión de información y autorización, por ejemplo, el principio de necesidad de conocer y los niveles de seguridad de información y clasificación de la información
c) La coherencia entre los derechos de acceso y políticas de clasificación de la información de los sistemas y redes;
d) La legislación pertinente y las obligaciones contractuales relativas a la limitación de acceso a los datos o servicios
e) La gestión de los derechos de acceso en un entorno distribuido y en red que reconoce todo tipos de conexiones disponibles;
f) La segregación de las funciones de control de acceso, por ejemplo, solicitud de acceso, autorización de acceso, administración de acceso;
g) Los requisitos para la autorización formal de las solicitudes de acceso
h) Los requisitos para la revisión periódica de los derechos de acceso;

i) La eliminación de los derechos de acceso;
j) El archivo de los expedientes de todos los acontecimientos importantes en relación con el uso y la gestión de identidades de usuario y la información secreta de autenticación;
k) Los roles con acceso privilegiado;

18.1.2. El acceso a las redes y los servicios de red

Los usuarios sólo deben disponer de acceso a los servicios de red y de la red que han sido específicamente autorizados para su uso.

Una política debe formularse en relación con el uso de redes y servicios de red. Esta política debe cubrir:

a) Las redes y los servicios de red que están autorizados a acceder;
b) Los procedimientos de autorización para determinar quién puede acceder a qué redes y servicios en red;
c) los controles y procedimientos para proteger el acceso a las conexiones de red y servicios de red de gestión;
d) Los medios utilizados para acceder a las redes y servicios de red
e) Los requisitos de autenticación de usuario para acceder a varios servicios de red;
f) el seguimiento de la utilización de los servicios de red.

La política sobre el uso de servicios de red debe ser compatible con el control de acceso de la organización política.

18.2. Gestión de acceso de los usuarios

Objetivo: Asegurar el acceso de los usuarios autorizados y para evitar el acceso no autorizado a los sistemas y servicios.

18.2.1. Registro de usuarios y bajas

Un proceso formal de registro de usuario y la cancelación de la matrícula debe ser implementado para permitir la asignación de los derechos de acceso.

El proceso de gestión de los ID de usuario debe incluir:

a) el uso de identificadores de usuario únicos para que los usuarios puedan estar vinculados y responsables de sus acciones; el uso de identificaciones compartidas sólo se permitirá cuando sean necesarias para el negocio u operativo razones y debe ser aprobado y documentado;
b) Inmediatamente desactivar o quitar los identificadores de usuario de los usuarios que han abandonado la organización;
c) La identificación y eliminación o desactivación del ID de usuario redundantes periódicamente;
d) Asegurarse de que los ID de usuario redundantes no se emiten a otros usuarios.

18.2.2. El acceso del usuario aprovisionamiento

Un proceso de provisión de acceso de usuario formal debe ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuario a todos los sistemas y servicios.

El proceso de aprovisionamiento para asignar o revocar los derechos de acceso concedidos a los ID de usuario debe incluir:

a) Obtener la autorización del propietario del sistema de información o servicio para el uso del sistema o servicio de información; aprobación por separado de derechos de acceso de gestión también puede ser apropiado;
b) Verificar que el nivel de acceso otorgado es adecuado a las políticas de acceso (ver 9.1) y es compatible con otros requisitos, tales como la separación de funciones;
c) Velar por que los derechos de acceso no están activados (por ejemplo, proveedores de servicios) antes de la autorización procedimientos se han completado;
d) El mantenimiento de un registro central de los derechos de acceso concedidos a un ID de usuario para acceder a los sistemas de información y los servicios;
e) La adaptación de acceso de los usuarios que han cambiado de roles o puestos de trabajo y la eliminación inmediata o bloqueando los derechos de acceso de los usuarios que han abandonado la organización;
f) Revisar periódicamente los derechos de acceso con los propietarios de los sistemas y servicios de información.

18.2.3. Gestión de derechos de acceso privilegiados

La asignación y utilización de los derechos de acceso privilegiado debe restringirse y controlarse.

La asignación de derechos de acceso privilegiado debe ser controlada a través de un proceso de autorización formal de acuerdo con la política de control de acceso correspondiente. Los siguientes pasos deben ser considerados:

a) Los derechos de acceso privilegiado asociados con cada sistema o proceso, por ejemplo, sistema operativo, base de datos sistema de gestión y cada aplicación y los usuarios a los que necesitan para ser asignados deben ser identificado;

b) Los derechos de acceso privilegiados debe asignarse a los usuarios en base a la necesidad de utilizar y en un evento-byevent base de acuerdo con la política de control de acceso, es decir, sobre la base de los requisitos mínimos por sus roles funcionales;
c) Deben mantenerse un proceso de autorización y un registro de todos los privilegios asignados. privilegiado los derechos de acceso no deben concederse hasta que el proceso de autorización se ha completado;
d) Requisitos para la expiración de los derechos de acceso privilegiado es preciso definir;
e) Derechos de acceso privilegiado se deben asignar a un ID de usuario diferente de los que se utilizan para regular de actividades empresariales. Actividades comerciales normales no se deben realizar a partir privilegiada ID;
f) Las competencias de los usuarios con derechos de acceso privilegiados deben revisarse periódicamente con el fin de verificar si están en consonancia con sus obligaciones;
g) Los procedimientos específicos deben establecerse y mantenerse para evitar el uso no autorizado de ID de usuario de administración de genéricos, de acuerdo a las capacidades de configuración de sistemas ";
h) Para los ID de usuario de administración genérica, la confidencialidad de la información secreta de autenticación debe ser mantenida cuando se comparte (por ejemplo, cambiar las contraseñas con frecuencia y tan pronto como sea posible cuando un privilegiado usuario abandona o cambia de empleo, comunicarlos entre los usuarios privilegiados con mecanismos adecuados).

18.2.4. Gestión de la información de autenticación de secreto de los usuarios

La asignación de la información secreta de autenticación debe ser controlada a través de un proceso oficial de gestión.

El proceso debe incluir los siguientes requisitos:

a) Los usuarios deben ser obligados a firmar una declaración para mantener la información de autenticación de secreto personal información de autenticación confidencial y secretos para mantener el grupo (es decir, compartido) únicamente en los miembros del grupo; esta declaración firmada se puede incluir en los términos y condiciones de empleo;
b) Cuando los usuarios están obligados a mantener su propia información secreta de autenticación deben ser prevista inicialmente con información segura temporal secreto de autenticación, que se ven obligados a cambiar en el primer uso;
c) Se establezca un procedimiento para verificar la identidad de un usuario antes de proporcionar nuevos, sustitutivos o información de autenticación temporal secreto;
d) La información temporal de autenticación secreta se debe dar a los usuarios de una manera segura; el uso de las partes externas o (texto sin cifrar) los mensajes de correo electrónico sin protección debe evitar;
e) La información de autenticación secreta temporal debe ser única para un individuo y no debe ser fácil de adivinar;
f) Los usuarios deben acusar recibo de la información secreta de autenticación;
g) Por defecto la información secreta de autenticación debe ser alterado después de la instalación de sistemas o software.

18.2.5. Revisión de los derechos de acceso de usuario

Los propietarios de activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.

La revisión de los derechos de acceso debe considerar lo siguiente:

a) Los derechos de acceso de los usuarios deben ser revisados a intervalos regulares y después de cualquier cambio, como la promoción, degradación o la terminación del empleo;

b) Los derechos de acceso de usuario deben ser revisados y asignados nuevamente cuando se pasa de un rol a otro dentro de la misma organización;
c) Las autorizaciones de derechos de acceso privilegiados deben revisarse a intervalos más frecuentes;
d) Las asignaciones de privilegios deben ser revisados periódicamente para asegurar que los privilegios no autorizados no se han obtenido;
e) cambios en las cuentas privilegiadas deben ser registrados para su revisión periódica.

18.2.6. La eliminación o el ajuste de los derechos de acceso

Los derechos de acceso de todos los empleados y los usuarios parte externa a la información y procesamiento de la información instalaciones deben ser retirados a la terminación de su empleo, contrato o acuerdo, o ajustada a cambio.

Tras la rescisión, los derechos de acceso de un individuo a la información y los activos asociados con instalaciones y servicios de procesamiento de la información deben ser removidos o suspendidos. Esto determinará si es necesario para eliminar los derechos de acceso. Los cambios de empleo deben reflejarse con la eliminación de todos los derechos de acceso dados inicialmente. Los derechos de acceso que deben estar eliminado o ajustado incluir los de acceso físico y lógico. La eliminación o el ajuste se pueden hacer por eliminación, la revocación o la sustitución de llaves, tarjetas de identificación, las instalaciones de procesamiento de información o suscripciones. Cualquier documentación que identifica los derechos de acceso de los empleados y contratistas debe reflejar el desmontaje y el ajuste de los derechos de acceso. Si un empleado que se marcha o externa usuario Parte haya contraseñas conocidas para los ID de usuario permanecen activas, éstas deben ser cambiadas después de la terminación o el cambio de empleo, contrato o acuerdo.

Derechos de acceso para la información y los activos asociados a las instalaciones de procesamiento de información deben ser reducido o eliminado antes de que caduque el empleo o cambios, dependiendo de la evaluación del riesgo factores tales como:

a) Si la terminación o el cambio es iniciado por el empleado, el usuario parte externa o por gestión, y la razón de la terminación;
b) Las responsabilidades actuales del empleado, el usuario parte externa o cualquier otro usuario;
c) El valor de los activos actualmente accesibles.

18.3. Responsabilidades del usuario

Objetivo: hacer que los usuarios sean responsables de salvaguardar su información de autenticación.

18.3.1. El uso de la información secreta de autenticación

Los usuarios deben estar obligados a seguir las prácticas de la organización en el uso de información secreta de autenticación.

Todos los usuarios deben ser advertidos de:

a) Mantener la información secreta de autenticación confidencial, asegurando que no es divulgada a ninguna otra parte, incluidas las personas de autoridad;
b) Evitar que se registrasen (por ejemplo, en papel, archivo de software o un dispositivo de mano) de autenticación secreta información, a menos que esto se puede almacenar de forma segura y el método de almacenamiento ha sido aprobado (por ejemplo, Caja fuerte de contraseñas);
c) Cambiar la información secreta de autenticación cuando se produzca algún indicio de su posible compromiso;

d) Cuando las contraseñas se utilizan como información de autenticación secreta, contraseñas de calidad seleccionados con suficiente longitud mínima que se encuentran:

    1. Fácil de recordar;
    2. No se basa en nada a otra persona, lo que podría fácilmente adivinar u obtener utilizando información relacionado a la persona, por ejemplo, nombres, números de teléfono y fechas de nacimiento, etc;
    3. No es vulnerable a los ataques de diccionario (es decir, no consisten de palabras incluidas en los diccionarios);
    4. Sin caracteres consecutivos idénticos, todos numéricos o todos alfabéticos;
    5. Si es temporal, cambiarlo en el primer inicio de sesión;

e) No compartir la información de autenticación secreta del usuario individual;
f) Garantizar una adecuada protección de las contraseñas cuando las contraseñas se utilizan como autenticación secreta, la información en los procedimientos de registro-en automatizadas y se almacenan;
g) No use la misma información secreta de autenticación para fines comerciales y no comerciales.

18.4. El control de acceso del sistema y la aplicación

Objetivo: evitar el acceso no autorizado a los sistemas y aplicaciones.

18.4.1. Restricción de acceso a la información

El acceso a las funciones de información y sistema de aplicación debe ser restringida de acuerdo con la política de control de acceso.

Restricciones de acceso deben basarse en las necesidades individuales de aplicaciones de negocio y de acuerdo con la política de control de acceso definido.

Lo siguiente debe ser considerado con el fin de apoyar los requisitos de restricción de acceso:

a) Proporcionar menús para controlar el acceso a las funciones del sistema de aplicación;
b) Controlar qué datos pueden ser accedidos por un usuario en particular;
c) El control de los derechos de acceso de los usuarios, por ejemplo, leer, escribir, borrar y ejecutar;
d) El control de los derechos de acceso de otras aplicaciones;
e) La limitación de la información contenida en los productos;
f) Proporcionar controles de acceso físicos o lógicos para el aislamiento de las aplicaciones sensibles, la aplicación datos o sistemas.

18.4.2. Asegure los procedimientos de entrada

Cuando lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones debe ser controlado por un procedimiento de inicio de sesión seguro.

Una técnica de autenticación adecuada debe ser elegido para justificar la identidad alegada de un usuario.

Cuando se requiere una autenticación y verificación de la identidad, los métodos de autenticación alternativa a las contraseñas, tales como medios criptográficos, tarjetas inteligentes, símbolos o medios biométricos, se debe utilizar.

El procedimiento para iniciar sesión en un sistema o aplicación debe ser diseñado para reducir al mínimo la oportunidad para el acceso no autorizado. Por tanto, el procedimiento de inicio de sesión debe revelar el mínimo de información sobre el sistema o la aplicación, con el fin de evitar la prestación de un usuario no autorizado con cualquier ayuda innecesaria. Un buen procedimiento de conexión debe:

a) No se muestren sistema o aplicaciones identificadores hasta que el proceso de inicio de sesión se ha completado con éxito;
b) Mostrar un aviso general advirtiendo que el equipo sólo debe tener acceso a los usuarios autorizados;
c) No dar mensajes de ayuda durante el proceso de inicio de sesión que ayudaría a un usuario no autorizado;
d) validar la información de inicio de sesión en sólo en la terminación de todos los datos de entrada. Si se presenta una condición de error, el sistema no debe indicar qué parte de los datos son correctos o incorrectos;
e) Proteger contra los intentos de inicio de sesión de fuerza bruta;
f) Registrar los intentos fallidos y exitosos;
g) Incrementar un evento de seguridad si se detecta un posible intento o violación con éxito de inicio de sesión de los controles;
h) mostrará la siguiente información en la finalización de un inicio de sesión exitoso:

    1. Fecha y hora del anterior inicio de sesión exitoso;
    2. Los detalles de cualquier intento de inicio de sesión fallidos desde el último éxito de inicio de sesión;

i) No se muestre una contraseña cuando se introduzcan;
j) No transmitir contraseñas en texto claro a través de una red;
k) Terminar las sesiones inactivas después de un período definido de inactividad, sobre todo en lugares de alto riesgo, como las áreas públicas o externas fuera de la gestión de seguridad de la organización o en los dispositivos móviles;
l) Restringir los tiempos de conexión para proporcionar seguridad adicional para aplicaciones de alto riesgo y reducir la ventana de oportunidad para el acceso no autorizado.

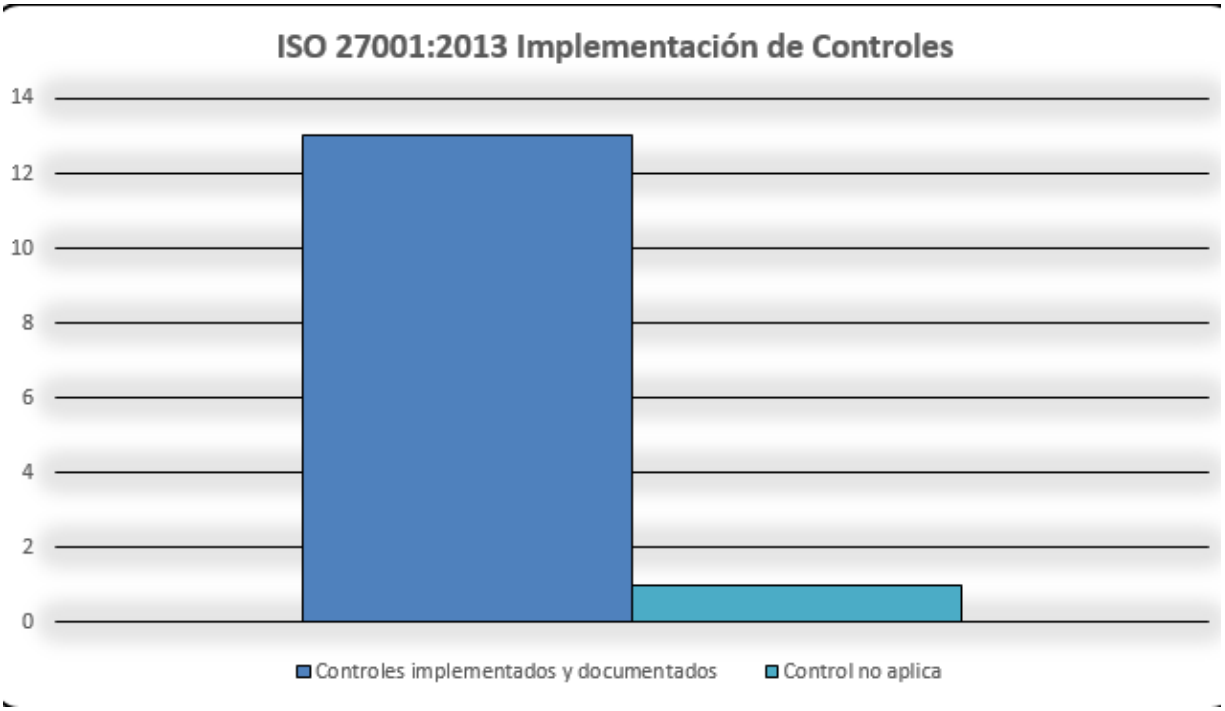
18.4.3. Sistema de gestión de contraseñas

Sistemas de gestión de contraseñas que deben ser interactivos y deben asegurarse de contraseñas de calidad.

Un sistema de gestión de contraseñas debe:

a) Aplicar el uso de identificadores de usuario y contraseñas individuales para mantener la rendición de cuentas;
b) Permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación de permitir errores de entrada;
c) Hacer cumplir una selección de contraseñas de calidad;
d) Obligar a los usuarios a cambiar sus contraseñas en el primer inicio de sesión;
e) Hacer cumplir los cambios regulares de contraseña y, según sea necesario;
f) Hacer cumplir los cambios regulares de contraseña y, según sea necesario;
g) No mostrar las contraseñas en la pantalla cuando se está introduciendo;
h) Almacén de contraseñas de archivos por separado de los datos de sistema de aplicación;
i) Almacenar y transmitir las contraseñas en forma protegida.

Estado de Spytech después la aplicación de los controles



Fuente: Elaboración Propia

Como se observa en la gráfica después de haber implementado los controles se evidencia que Spytech cuenta con un 93% de cumplimiento con la Norma y su estándar garantizando así la confidencialidad, disponibilidad, integridad, minimizando así el riego y evitando que las amenazas se materialicen.

19. HARDWARE PARA EN CONTROL DE ACCESO

Los sistemas de control de acceso actualmente no permiten tener el control de entrada y salida de forma automatizada del personal de una organización a las áreas sensibles. El control de acceso cuenta con un lector biométrico de huella dactilar y teclado para acceder al lugar restringido mediante clave y huella. Este dispositivo está dotado de teclado y pantalla LCD y la identificación está basada en la identificación de huellas dactilares, usuario y contraseña. Este sistema le permite a la entidad configurar y administrar el sistema desde la red corporativa o desde internet, la información se da en tiempo real, toda la información entre el sistema de control y la red son encriptados para brindar mayor seguridad a los usuarios.

Para SPYTECHT se implementará un hardware Biostation Suprema, este sistema cuenta con dos métodos de autenticación uno por huella y el otro por clave, lo que nos brinda un mayor nivel de seguridad a la hora de habilitar el acceso al sitio, esto también necesita evita la suplantación de la huella.

Ver la información técnica ver Anexo A - DataSheet-Biostation

CONCLUSIONES

La implementación de controles de acceso a áreas con información sensible le permite a Spytech mantener un nivel de seguridad alto en el acceso a la información.

La implementación de los controles de seguridad le permite a Spytech controlar los riesgos de perdida, daño, robo de la información.

Los controles aplicados para Spytech son las mejores prácticas de fácil adaptación que en conjunto con acciones adicionales implementadas como el monitoreo, evaluación y mejora continua minimiza el riesgo y evita que se materialice las amenazas.

20. BIBLIOGRAFÍA

[1] NORMA INTERNACIONAL ISO/IEC 27002 - TECNOLOGIA DE LA INFORMACION –TENCICAS DE SEGURIDAD- CODIGO PARA PRACTICAS DE CONTROLES DE LA INFORMACION.

[2] INTERNACIONAL ESTANDAR – ISO/IEC 27000 – TECNOLOGIA DE LA INFORMACION – TECNICAS DE SEGURIDAD – SISTEMAS DE GESTION DE SEGURIDAD DE LA INFORMACION – INFORMACION GENERAL Y VOCABLURARIO.

TECNOLOGIA DE LA INFORMACION ISO/IEC 27001: 2013 - TECNICAS DE SEGURIDAD – SISTMAS DE GESTION DE LA SEGURIDAD DE LA INFORMACION – REQUISITOS.

21. **ANEXO A.** DATA SHEET- BIOSTATION

biostation

Innovative Fingerprint Terminal

2.5" 16M Color LCD
Display messages, video, animation and photos to convey various information and notices

Wi-Fi Wireless LAN
Easy network integration and data transfer from PC using wireless network without cabling

Industry leading fingerprint identification speed and capacity
Identify 3,000 fingerprints in 1 second and store maximum 50,000 fingerprints and 500,000 events in internal memory

USB memory slot
Easy data transfer to PC or other BIOSTATIONs using a USB memory device

High quality sound
16 bit Hi-Fi sound for background music, sound effect and voice instruction.

Applications

- Time attendance and access control for offices
- Integrated payroll and HR management of employees
- Networked security for IBS buildings, financial and research institutes
- Data collection for customer reward management

Model Information

Product Type	Fingerprint Sensor		
	OC(optical)	TC(capactive)	FC(thermal)
Basic Model	BST-OC	BST-TC	BST-FC
Wireless option	BSTW-OC	BSTW-TC	BSTW-FC
RF option	BSR-OC	BSR-TC	NA
Wireless + RF	BSRW-OC	BSRW-TC	NA

Specifications

- CPU : Dual CPU (32bit RISC + 400MHz DSP)
- Memory : 72MB flash + 34MB RAM
- Display : 2.5" QVGA 16M Color LCD
- Fingerprint identification speed : 3,000 match in 1 second
- Fingerprint capacity : 50,000 fingerprint templates
- Log capacity : 500,000 events
- RF card : 125KHz proximity (optional)
- Network interface : Wireless LAN (optional), TCP/IP, RS485
- PC interface : USB, RS232
- USB memory slot : USB Host
- Output relay : Deadbolt, EM lock, door strike, automatic door
- Wiegand I/O, 4 TTL I/O
- Microphone and speaker for door phone
- Navigation key for menu movement
- 4 Function keys for user-defined functions
- Operation modes : Fingerprint, PIN, PIN + Fingerprint, Card, Card + Fingerprint, Card + PIN (RF model)
- Size : 135 x 128 x 50mm (W x H x D)

For Sales and Inquiries, Please Contact:

Suprema Inc.
16F Parkview Office Tower, Jeongja-dong, Bundang
Seongnam, Gyeonggi, 463-863 Korea
- Tel : +82-31-783-4502, Fax : +82-31-783-4503
- E-mail : sales@supremainc.com
- Homepage : http://www.supremainc.com

SUPREMA