PROPUESTA DE MEJORAS PARA LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES.

PROPOSAL FOR IMPROVEMENTS TO THE INFORMATION SECURITY POLICIES OF THE LOS LIBERTADORES UNIVERSITY FOUNDATION.

Luis Fernando Avellaneda Avellaneda
Edgar Antonio Carreño Chaparro
Wilmer Enrique Hernández Paez

Héctor Manuel Herrera Herrera

RESUMEN

Con este proyecto queremos identificar y analizar algunas políticas de Seguridad que se están aplicando en la Fundación Universidad Los Libertadores con relación a la norma ISO 27001 (**NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27001-2013**), y según los hallazgos encontrados propondremos mejoras a nivel de procedimientos, seguimientos y normatividad.

Partiremos de lo que existe actualmente en la Institución a nivel de seguridad y con guía de la ISO 27001 del 2013, realizaremos nuevas propuestas o sugerencias sobre temas que se deban y puedan aplicar a la universidad, siempre en pro de mejora de la seguridad de la Información a nivel del

área de Informática, y del beneficio institucional eliminando posibles brechas de seguridad y vulnerabilidades que se puedan encontrar.

ABSTRACT

With the project, we want to identify and analyze some security policies that are being applied in the Fundación Universitaria Los Libertadores about the ISO 27001 standard (NTC-ISO-IEC COLOMBIANA 27001-2013), and according to the findings, we will propose improvements at the level of procedures, monitoring, and regulations.

We will start, with that currently exists in the institution, in terms of security and with the guidance of ISO 27001 of 2013, of new suggestions or proposed topics that should and can be applied to the university, always in favor of improving information security at the level of the IT area, and the institutional benefit by eliminating possible security gaps and vulnerabilities that can be found.

INTRODUCCIÓN

Con el continuo cambio tecnológico, la creación de constantes aplicaciones y nuevas Apps para los diferentes sectores de la sociedad (Educativo, Laboral, Económico, Científico, Salud), el fácil acceso a códigos de programación y la forma de poder adquirir este conocimiento de una manera práctica, hace que al igual que obtener grandes beneficios y el cubrir varias necesidades tecnológicas a las diferentes instituciones o empresas, surja de manera exponencial riesgos y amenazas para las mismas, afectando el activo más valioso que se puede tener hoy en día, la Información.

Teniendo conocimiento sobre las nuevas amenazas que nacen a diario en el Ciberespacio, se ve la

necesidad de aplicar políticas que ayuden a blindar y cuidar la información evitando que una amenaza se pueda materializar.

Es por este motivo que deseamos enfocarnos en conocer algunas de las políticas de Seguridad que utiliza la Fundación Universidad los Libertadores y entregar sugerencias de posibles mejoras de acuerdo a la Norma ISO 27001-2013.

Pregunta

¿Se está aplicando de forma correcta las políticas de Seguridad de la Información de acuerdo a lo propuesto en la norma ISO 27001-2013 en la institución Universitaria los Libertadores?

Objetivo general

Detectar posibles vulnerabilidades en las actuales políticas de seguridad de la información de la fundación universitaria Los Libertadores en el área de Informática, con el fin de poder proponer mejoras en torno al buen funcionamiento y aseguramiento de la información de acuerdo a la norma ISO 27001 -2013.

Objetivos específicos

- Identificar las políticas y procedimientos de seguridad que está aplicando actualmente la Universidad los Libertadores sobre los sistemas de información.
- Proponer políticas y procedimientos existentes en la norma ISO 27001-2013, que no hayan

sido visibles o detectadas por la institución y que puedan ser aplicables para una mejora continua a nivel de Seguridad de la Información.

- Analizar y comparar las actuales políticas de la universidad VS la propuesta desarrollada en el proyecto.

Alcance

Generar una propuesta a la Institución Fundación Universitaria los Libertadores donde se busque mejorar las políticas de seguridad de la información a nivel de Gestión de Activos de la Información, control de acceso y Seguridad de los Recursos Humanos tomando como referencia la norma ISO 27001 -2013, crear conciencia sobre las diferentes vulnerabilidades que se pueden generar al no tener un correcto control sobre estas políticas y la importancia de aplicar sistemas de seguridad a nivel del área Informática.

REFERENTES TEÓRICOS

En el proceso de encontrar mejoras o sugerencias a los procesos y procedimientos que se están aplicando actualmente en la Universidad los libertadores en los temas referentes a Políticas de Seguridad, tenemos como guía la documentación entregada por los Ingenieros Mack Freddy Eusseler Vela (Gerente de Tecnología de la Universidad los Libertadores), y Gisselle Bueno Meriño (Jefe de Infraestructura TICs). (Fundacion Universitaria los Libertadores, 2017)

Para iniciar el proceso de conocimiento y análisis de las políticas aplicadas, y compararlas contra las políticas de la norma ISO 27001- 2013.

Documentación adquirida aplicada en la Universidad los Libertadores.

- Politica-datos-personales-2019-2

- Politica-seguridad-informacion-2019-2
- Gt-pr-006 Gestión de Acceso de Usuarios

Documentación sobre Políticas y Seguridad de la Información.

- NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27001- 2013

Antecedentes y Estado del Arte

Entre la documentación encontrada como referencia nos guiamos de trabajos relacionados con un enfoque similar a temas de seguridad.

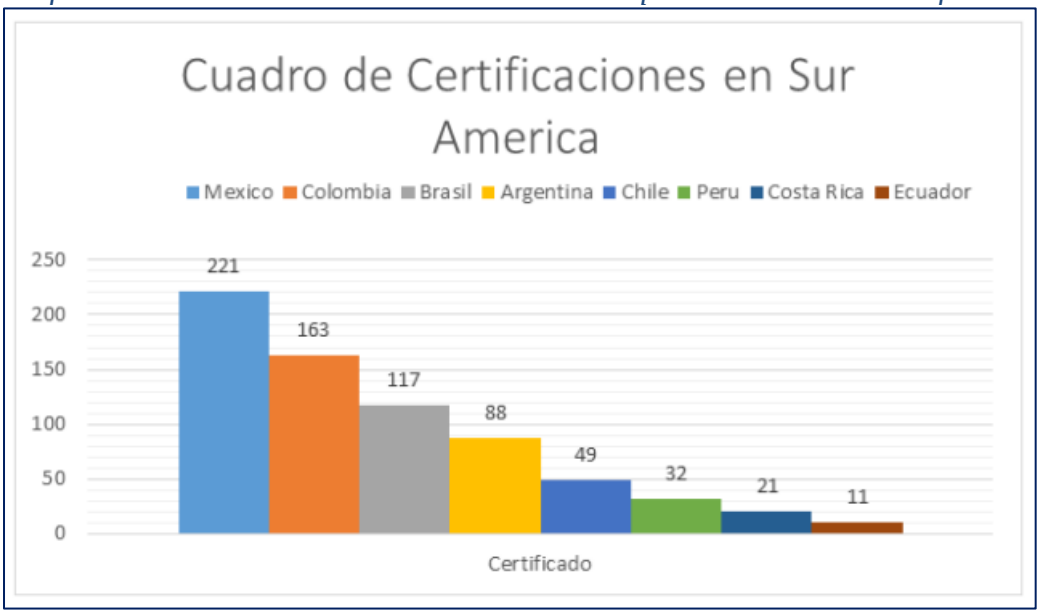
1. Políticas de gestión de seguridad de la información, fundamentadas en la norma ISO/IEC 27001, centro de datos diseñado con el estándar ANSI/TIA 942

En el presente documento los investigadores realizan un análisis sobre el estándar ANSI/TIA 942 el cual contiene diferentes numerales que se deben tener en cuenta en el momento de construcción de un centro de datos, estos numerales van desde estándares para su correcta elaboración, infraestructura, cableado estructurado, refrigeración y demás aspectos importantes a la hora de emprender dicha labor. Pero se dieron cuenta que no se tiene ningún apartado que les ayude con las políticas de seguridad de la información en las cuales puedan contribuir a la correcta protección de la confidencialidad, integridad y disponibilidad de la información.

Por ello se dieron a la tarea de realizar una investigación muy puntual sobre que norma o estándar existente les ayudaría con dicha labor, y es allí donde se centraron en la norma ISO 27001 -2013 la cual iba a servir como base para el planteamiento de dichas políticas, adicional en las

investigaciones realizadas se dieron cuenta que en Latinoamérica existe gran variedad de empresas que se encuentran certificadas en ISO27001 y que esto ha ayudado que los SGSI (sistema de gestión de seguridad de la información) de las compañías sean cada vez más robustos. A continuación, una gráfica de lo encontrado por los autores del presente escrito.

Gráfica 1. Resumen Entidades de Latinoamérica que se encuentran Certificadas.



Fuente*: Políticas de gestión de seguridad de la información, fundamentadas en la norma ISO/IEC 27001, centro de datos diseñado con el estándar ANSI/TIA 942*

Como se puede observar y fue algo que los investigadores detallaron es que en Ecuador que es uno de los países de su interés no existen muchas compañías que sean certificadas y por ende el estándar de la norma ISO no es muy utilizado. Esto les ayudo a que precisamente quisieran orientar sus políticas a dicha norma y que de una u otra manera lograran unificar políticas tanto con los apartados que se mencionan en ANSI como con los controles existentes en la norma ISO.

Para finalizar cabe mencionar que uniendo estos dos marcos de referencia lograron crear políticas de seguridad de la información para el área de telecomunicaciones, infraestructura, sistema eléctrico, sistema mecánico de un centro de datos. Dichas políticas incluyen el monitoreo constante de los sistemas, identificación de activos, zonas delimitadas de cargue y descargue, protección

contra accesos a personal no autorizado y demás puntos que podemos encontrar en el anexo A de la norma ya mencionada (César Wilfrido Astudillo-García, 2019).

2. Políticas de Seguridad de la Información para la Universidad la Gran Colombia.

En este proyecto se toma como base la falta de políticas de seguridad para la protección de los activos tanto físicos como lógicos.

En el planteamiento podemos observar la ausencia de directrices hacia la norma de seguridad para la protección de los activos físicos y de la información, y evitar ataques internos o externos que se puedan presentar.

Por esta razón se planteó como objetivo general "proponer políticas de seguridad de la información para la universidad la gran Colombia con el fin de proteger los activos de la institución, asegurando la confidencialidad, integridad y disponibilidad de la información involucrando a las personas que para estas sean aplicadas en desempeño de sus funciones".

Y el alcance del mismo proyecto es, "Este proyecto se aplicará a todas las dependencias que conforman la universidad La Gran Colombia, debe dársele cumplimiento, por todos los empleados, proveedores y personal externo, que desempeñe alguna labor o proporciones algún tipo de servicio dentro de ella. Estará enmarcada dentro de los parámetros de los conocimientos adquiridos en el módulo de Ingeniería Forense y Gestión de la seguridad.

No se trata de herramientas técnicas sino de una serie de normas que contribuyen a subir el nivel de seguridad de la universidad y podrá sufrir modificaciones futuras, de acuerdo a los requerimientos del momento".

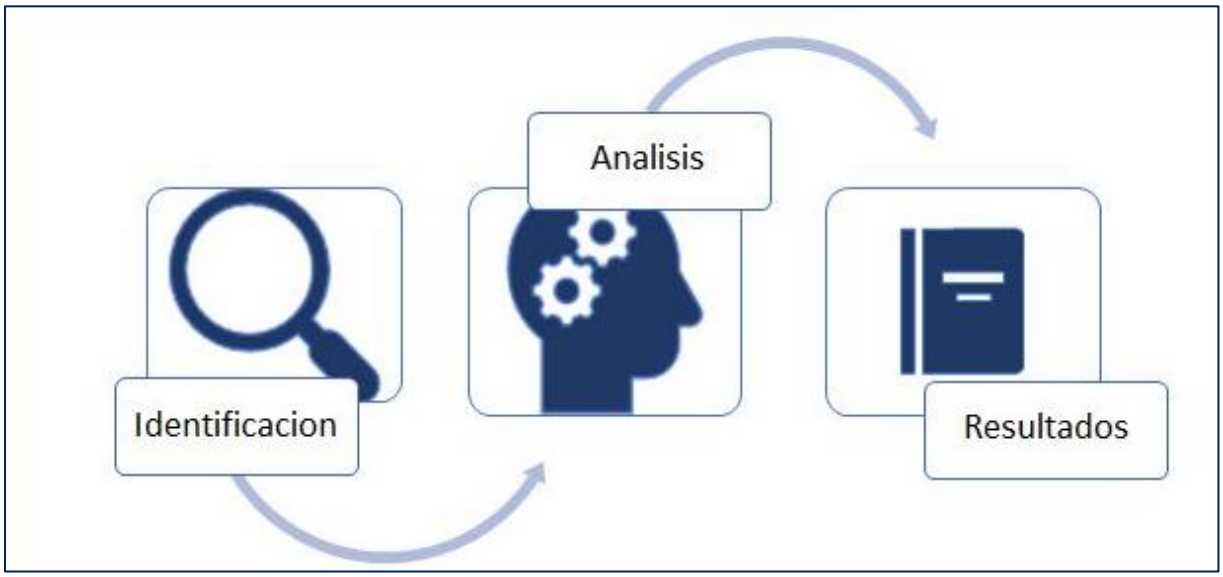
Con este análisis podemos entender que siempre se busca la mejora a nivel de seguridad en todos los aspectos y en las diferentes entidades existentes independiente de su Core de negocio, Financiero, Textil, Comercial, Educativo, Minero; las entidades cada vez son más conscientes de la importancia de cuidar y proteger su mayor activo que es la Información. (Yuri Xiomara Becerra Rozo, 2022)

Metodología.

La Metodología que se utiliza en este trabajo de investigación está basado con un enfoque Cualitativo que nos permite realizar la investigación y descripción de la información referentes a las políticas de seguridad de la información de la institución Universitaria los Libertadores.

La finalidad de la investigación es plantear unas mejoras a nivel de políticas de la seguridad de la información basándonos en el Norma ISO 27001 – 2013, los pasos aplicados en esta metodología son:

Gráfica 2. Metodología



Fuente 1: El Autor

1. Identificación

En esta fase inicial del proyecto se pretende realizar la recolección de las políticas de seguridad de la información con las que actualmente cuenta la Fundación Universitaria los Libertadores, después de ello poder identificar las diferentes falencias que puedan contener y adicional poder captar de una forma más precisa aquellas vulnerabilidades a las que podría estar expuesta la institución por el hecho de no contar con políticas de seguridad definidas de manea adecuada y que podría conllevar a la materialización de riesgos que afecten directamente la confidencialidad, integridad y disponibilidad de la información y afectando a los estudiantes y demás personal que pertenezca a la Institución.

2. Análisis

En la segunda fase de nuestro proyecto se busca realizar el análisis y comparación de las políticas de seguridad de la información con las que cuenta la fundación universitaria los libertadores contra las dispuestas por la ISO 27001 de 2013, y más que comparar políticas se desea analizar cuáles son los controles que se deberían implementar para una correcta gestión del SGSI de la universidad. Adicional se pretende realizar el análisis de un modelo GAP que nos ayude a identificar cuáles son las vulnerabilidades que se puedan materializar y afectar los sistemas de información de la institución.

Cabe mencionar que nos basaremos en 3 puntos específicos de las políticas de seguridad de la información que se encuentran descritos tanto en la ISO como en la universidad, las políticas para analizar son:

a. Seguridad en los recursos humanos
b. Gestión de activos de información
c. Control de accesos

3. Resultados

Como tercer y última fase tenemos los resultados en los cuales se pretende mostrar la propuesta que busca mejorar las políticas de seguridad de la información existentes en la universidad, de llegar a implementarse podrían ser un gran aporte para proteger la confidencialidad, integridad y disponibilidad de la información en la institución.

Se realiza y entrega un análisis de las Políticas, objetivos, y mejoras de implementación para cada uno de los controles que se van a evaluar de acuerdo a la norma ISO 27001-2013.

ANÁLISIS Y RESULTADOS

Análisis GAP o Análisis de Brechas

Con este análisis se pretende determinar cual es el estado actual de las políticas de seguridad de la información con las que cuenta la institución y así lograr identificar las falencias existentes. Con el fin de obtener un punto de partida (¿Dónde estamos?) en cada política propuesta, y una meta (¿dónde queremos estar?). (TuDashboard, 2021)

A continuación, se presenta el estado de los controles descritos en la política de seguridad de la información de la institución.

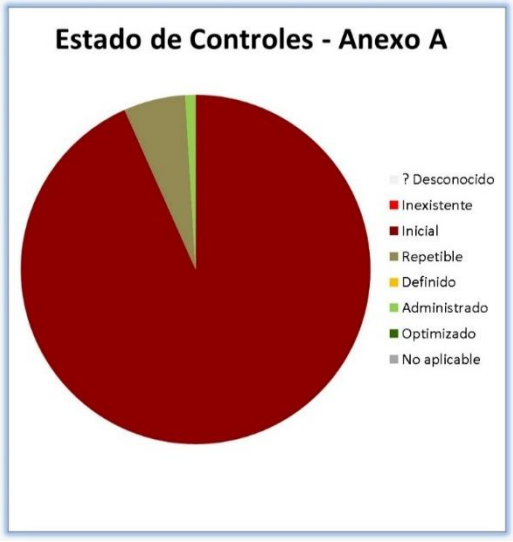
Tabla 1. Control y Estado actual de las Políticas Norma ISO 27001-2013

ITEM	CODIGO	CONTROL	ESTADO ACTUAL
1	A7.1.1	Investigación de antecedentes - (Selección)	Inicial
2	A7.1.2	Términos y condiciones del empleo	Inicial
3	A7.2.1	Responsabilidades de gestión	Inicial
4	A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Repetible
5	A7.2.3	Proceso disciplinario	Inicial
6	A7.3.1	Responsabilidades ante la finalización o cambio	Inicial
7	A8.1.1	Inventario de activos	Inicial
8	A8.1.2	Propiedad de los activos	Repetible
9	A8.1.3	Uso aceptable de los activos	Inicial
10	A8.1.4	Devolución de activos	Inicial
11	A8.2.1	Clasificación de la información	Repetible

12	A8.2.2	Etiquetado de la información	Inicial
13	A8.2.3	Manipulado de la información	Inicial
14	A8.3.1	Gestión de soportes extraíbles	Inicial
15	A8.3.2	Eliminación de soportes	Inicial
16	A8.3.3	Soportes físicos en tránsito	Inicial
17	A9.1.1	Política de control de acceso	Administrado
18	A9.1.2	Acceso a las redes y a los servicios de red	Inicial
19	A9.2.1	Registro y baja de usuario	Repetible
20	A9.2.2	Provisión de acceso de usuario	Repetible
21	A9.2.3	Gestión de privilegios de acceso	Repetible
22	A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Inicial
23	A9.2.5	Revisión de los derechos de acceso de usuario	Inicial
24	A9.2.6	Retirada o reasignación de los derechos de acceso	Inicial
25	A9.3.1	Uso de la información secreta de autenticación	Inicial
26	A9.4.1	Restricción del acceso a la información	Inicial
27	A9.4.2	Procedimientos seguros de inicio de sesión	Inicial
28	A9.4.3	Sistema de gestión de contraseñas	Inicial
29	A9.4.4	Uso de utilidades con privilegios del sistema	Inicial
30	A9.4.5	Control de acceso al código fuente de los programas	Inicial

Fuente 2: Qué es el análisis GAP. (https://tudashboard.com/analisis-gap/)

Gráfica 3. Estados de Controles - Anexo A



Fuente 3: Fuente: Qué es el análisis GAP. (https://tudashboard.com/analisis-gap/)

En la tabla presentada anteriormente podemos encontrar el análisis que se realiza a las políticas de seguridad de la información dispuestas para la Fundación Universitaria Los Libertadores, en dicha investigación podemos identificar el estado de los controles aplicados dentro de la institución y validar las posibles mejoras que se podrían aplicar para aumentar el nivel de dicho estado.

Este procedimiento se realiza en tres lineamientos seleccionados en el presente proyecto (Gestión de activos, control de accesos, y seguridad de los recursos humanos) en los cuales existen falencias que deberían ser corregidas, ya que en cada uno de ellos se identificó la redacción de un documento referente a la política de seguridad de la información, pero no existen documentos que soporten el proceso que se realiza.

Al finalizar la identificación y estado de cada uno de los controles se logra obtener como resultado que el **93%** se encuentran en estado inicial, **6%** en estado repetible y **1%** en estado administrado, teniendo en cuenta dicho análisis se determina y se evalúan propuestas de mejoras para cada uno de los controles seleccionados.

Tabla 2. Descripción de los Estados

Estado	Significado	Proporción de requerimientos SGSI	Proporción de Controles de Seguridad de la Información
? Desconocido	No ha sido verificado	0%	0%
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	0%	0%
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	100%	93%
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	0%	6%
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	0%	0%
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	0%	1%
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	0%	0%
No aplicable	A fin de certificar un SGSI ,todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	0%	0%

Fuente 4: Cuadro ISO 27001 y controles GAP

Tabla 3. Estado Actual Vs Estado Esperado

ITEM	CODIGO	CONTROL	ESTADO ACTUAL	MEJORAS	ESTADO ESPERADO
1	A7.1.1	Investigación de antecedentes - (Selección)	Inicial	Se propone el cumplimiento de los diferentes Controles descritos en esta política, la única finalidad es proteger la	Administrado
2	A7.1.2	Términos y condiciones del empleo	Inicial		Administrado
3	A7.2.1	Responsabilidades de gestión	Inicial		Administrado

4	A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Repetible	información sobre posibles amenazas que se puedan realizar por medio del Ser Humano.	**Administrado**
5	A7.2.3	Proceso disciplinario	Inicial		**Administrado**
6	A7.3.1	Responsabilidades ante la finalización o cambio	Inicial		**Administrado**
7	A8.1.1	Inventario de activos	Inicial	Teniendo en cuenta lo descrito en la norma ISO 27001:2013 se construye un procedimiento que permita realizar el levantamiento de activos de información, identificación de dueños de los activos, clasificación y etiquetado de los mismos.	**Administrado**
8	A8.1.2	Propiedad de los activos	Repetible		**Administrado**
9	A8.1.3	Uso aceptable de los activos	Inicial		**Administrado**
10	A8.1.4	Devolución de activos	Inicial		**Administrado**
11	A8.2.1	Clasificación de la información	Repetible		**Administrado**
12	A8.2.2	Etiquetado de la información	Inicial		**Administrado**
13	A8.2.3	Manipulado de la información	Inicial		**Administrado**
14	A8.3.1	Gestión de soportes extraíbles	Inicial		**Administrado**
15	A8.3.2	Eliminación de soportes	Inicial		**Administrado**
16	A8.3.3	Soportes físicos en tránsito	Inicial		**Administrado**

ITEM	CODIGO	CONTROL	ESTADO ACTUAL	MEJORAS	ESTADO ESPERADO
17	A9.1.1	Política de control de acceso	Administrado	Teniendo los controles descritos dentro del numeral A9 de la norma ISO 27001:2013 se propone una metodología para	**Optimizado**
18	A9.1.2	Acceso a las redes y a los servicios de red	Inicial		**Optimizado**

19	A9.2.1	Registro y baja de usuario	Repetible	tener un mejor manejo de control de accesos dentro de la institución.	**Optimizado**
20	A9.2.2	Provisión de acceso de usuario	Repetible		**Optimizado**
21	A9.2.3	Gestión de privilegios de acceso	Repetible		**Optimizado**
22	A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Inicial		**Optimizado**
23	A9.2.5	Revisión de los derechos de acceso de usuario	Inicial		**Optimizado**
24	A9.2.6	Retirada o reasignación de los derechos de acceso	Inicial		**Optimizado**
25	A9.3.1	Uso de la información secreta de autenticación	Inicial		**Optimizado**
26	A9.4.1	Restricción del acceso a la información	Inicial		**Optimizado**
27	A9.4.2	Procedimientos seguros de inicio de sesión	Inicial		**Optimizado**
28	A9.4.3	Sistema de gestión de contraseñas	Inicial		**Optimizado**
29	A9.4.4	Uso de utilidades con privilegios del sistema	Inicial		**Optimizado**
30	A9.4.5	Control de acceso al código fuente de los programas	Inicial		**Optimizado**

Fuente 5: Cuadro ISO 27001 y Controles GAP

En este artículo "**Propuesta de mejoras para las políticas de seguridad de la información de la Fundación Universitaria los Libertadores**" se describe en el cuadro anterior cual es el estado actual de madurez de los controles en la Fundación Universitaria los Libertadores, cuáles son las mejoras que se describe en el presente documento y por último el estado al que se pretende llegar si la universidad decide implementar cada uno de los controles y estrategias descritas.

Cabe mencionar que lo ideal es que la entidad Universitaria siga cada uno de los pasos que se describen con ello el sistema de gestión de seguridad de la información se fortalece y se mitigan

brechas de seguridad existentes.

A.7 Seguridad de los Recursos Humanos

La finalidad u objetivo de esta política es, Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

A.7.1 Antes de asumir el empleo

Objetivo. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

Entre los controles que se pueden aplicar están la verificación de antecedentes de las personas que están participando al puesto, analizar los soportes que por Ley se puedan exigir para conocer algo de aspectos a nivel social, teniendo en cuenta el perfil para el cual se desea contratar al individuo.

Cuando haya sido contratada la persona para el cargo, deben existir acuerdos contractuales para establecer las responsabilidades de acuerdo a la seguridad de la Información y su uso.

A.7.2 Durante la ejecución del empleo

Objetivo. Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

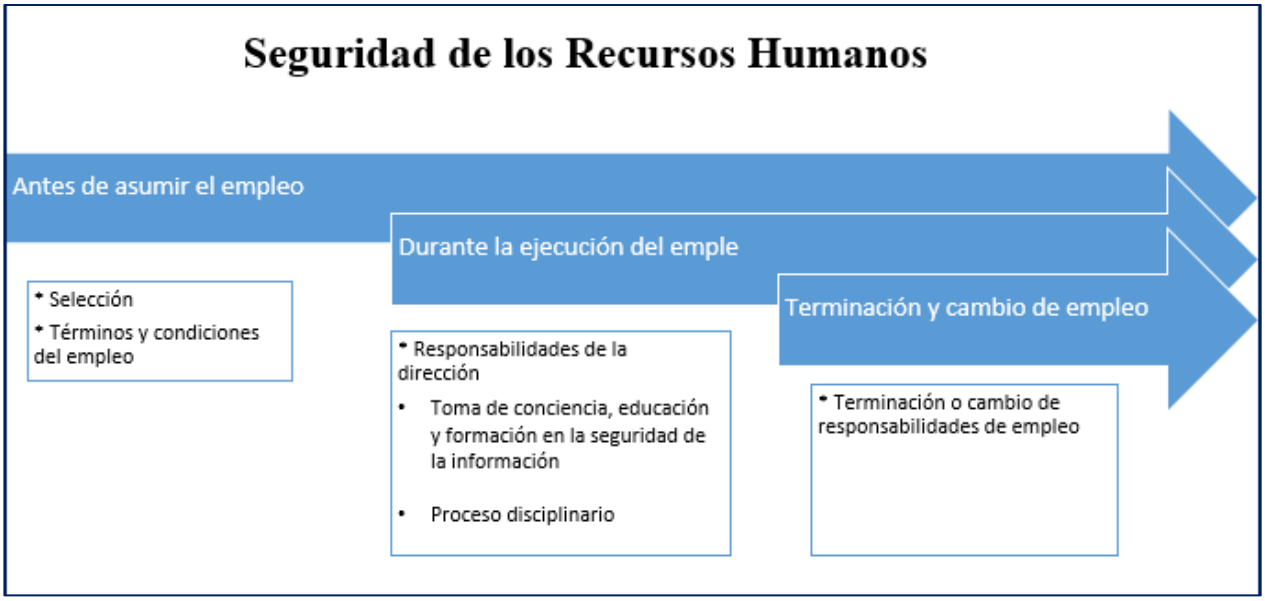
Entre los controles se le debe exigir a todos los empleados (directos o Contratistas) la aplicación de la seguridad de la Información de acuerdo a las políticas de la organización, se debe capacitar, educar y concientizar a todo el personal sobre la importancia de la seguridad con la información y las sanciones que puede recibir por faltar a este deber que acepto cuando ingreso a la Institución.

A.7.3 Terminación y cambio de empleo

Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.

Se debe tener claridad sobre la importancia de mantener la seguridad y Confidencialidad sobre la información de la Universidad aun si ya no está laborando en la institución. (Icontec Internacional, 2013)

Gráfica 4. Política Seguridad de los Recursos Humanos



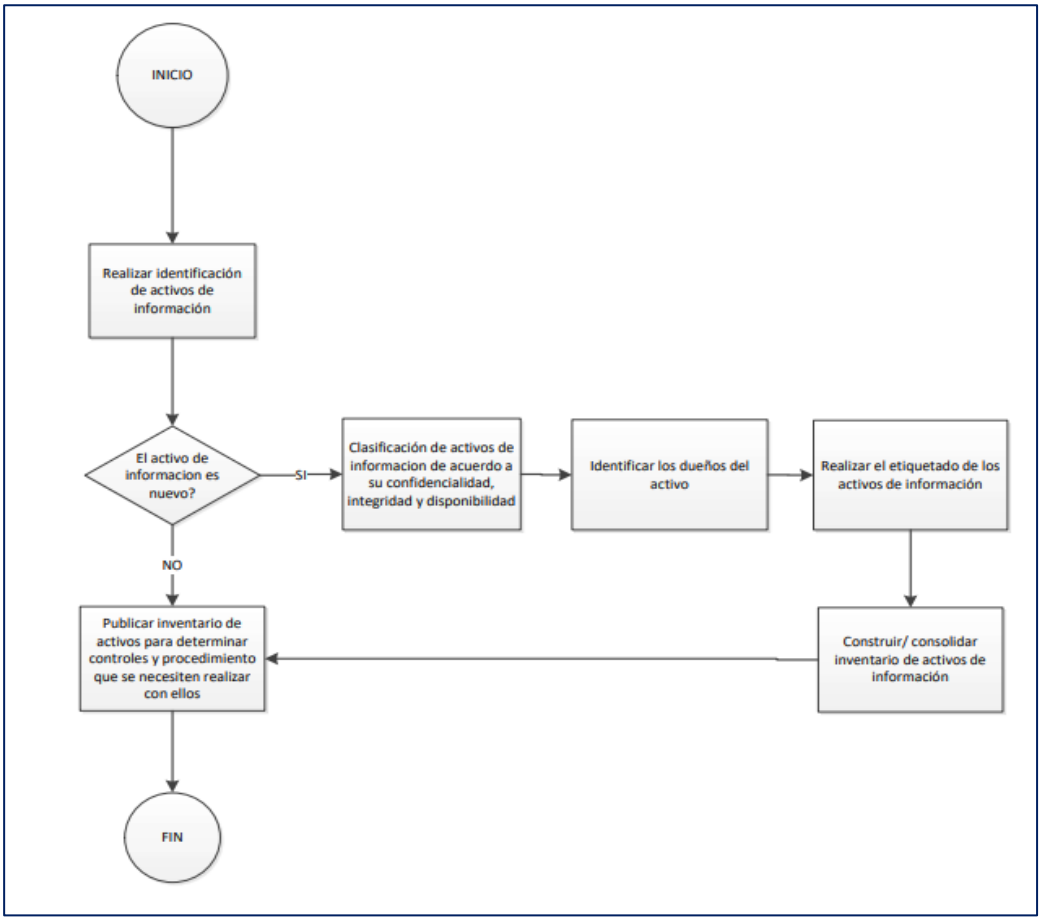
Fuente 6: El Autor

Gestión de activos de información.

Una de las mejoras frente a las políticas de seguridad de la información que se proponen en el presente documento es la implementación de políticas de gestión de activos, en el documento suministrado por la universidad se pudo identificar que no se realiza un adecuado inventario de activos de información, por ende es necesario implementar un procedimiento el cual ayude a fundamentar de manera adecuada cada uno de los pasos a seguir para realizar dicha labor.

Dentro de la norma ISO 27001 se establece en su anexo A.8 que se debe generar un inventario de activos de información, se debe realizar la identificación y clasificación de la información, adicional de contar con un etiquetado o estandarización que permita saber cuáles son los activos más valiosos para la institución y poder establecer controles que sirvan para la protección de los mismos.

Gráfica 5. Diagrama Gestión de Activos

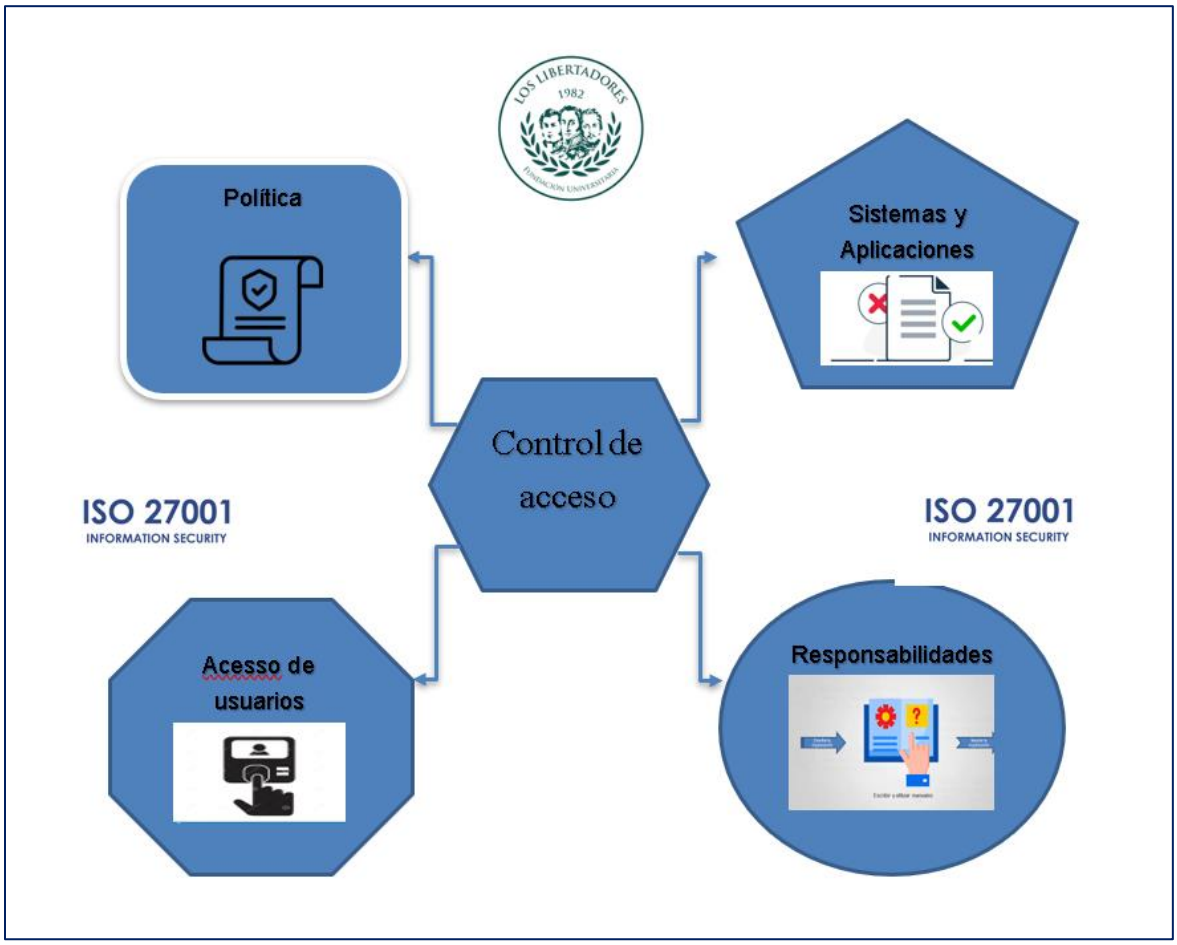


Fuente 7: El Autor

Control de acceso

Este es un elemento de la seguridad esencial que determina quien tiene permisos para acceder a determinados datos, aplicaciones y recursos. Las directivas del control de acceso protegen los espacios digitales, estos dependen en gran medida de técnicas como autenticación y la autorización, que permiten a las organizaciones verificar de forma explícita que los usuarios son quienes dicen ser y que cuentan con el nivel adecuado de acceso con base en elementos contextuales como el dispositivo, la ubicación, el rol y mucho más, todo esto bajo los objetivos y controles de referencia de la norma ISO 27001-2013 (Mintic, 2022).

Gráfica 6. Proceso Control de Accesos[o]



Fuente 8: El Autor

- **A 9.1.1 Política de control de acceso**

El objetivo es garantizar que la información, las áreas de procesamiento de información, las redes de datos, los recursos de la plataforma tecnológica y los sistemas de información de la fundación universitaria los libertadores estén debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico y físico

Es prioritario definir el personal que tenga acceso a información sensible, por lo cual limita el acceso de usuarios de aplicaciones computarizadas únicamente a funcionarios y estudiantes que tengan que ver directamente con sus responsabilidades y funciones a cargo, debido a que la información puede ser sensible o tener un carácter confidencial. Así mismo es necesario restringir

el acceso a las instalaciones donde dicha información se encuentra guardada, garantizando así la confidencialidad e integridad de la misma.

- **A 9.3 Responsabilidades de los usuarios**

Las responsabilidades de todos los usuarios es ser conscientes de sus responsabilidades durante el mantenimiento de controles de acceso eficientes, en particular respecto a la utilización y buen manejo de las contraseñas y la seguridad en cada uno de los sistemas de información de la institución.
Una buena estrategia es definir y documentar de forma clara las responsabilidades relativas a la seguridad de la información en las descripciones o perfiles como por ejemplo:

- Los usuarios y contraseñas son de uso personal, el cual es intransferible
- Cualquier incidente o mínima sospecha que afecte la confidencialidad, integridad o disponibilidad de la información es necesario reportarlo con el área o personal encargado de seguridad de la información de la institución
- Por seguridad y buenas prácticas todo usuario con acceso a los sistemas de información deberá cambiar su contraseña con una frecuencia mínima de 6 meses. (Mintic, 2022)

A 9.4 Control de acceso a sistemas y aplicaciones

Sugerir procedimientos para la asignación de acceso a los sistemas, bases de datos, aplicativos y servicios de información, la solicitud y aprobación de acceso a Internet o redes externas; el uso de computación móvil y trabajo remoto.

A 9.2 Gestión de Acceso de usuarios

Este elemento de la seguridad es la que determina quien tiene permisos para acceder a determinados datos, aplicaciones y recursos, las directivas de control de acceso dependen en gran medida de técnicas como la autenticación y la autorización.

En este enfoque, la administración de privilegios en los dispositivos y cuentas informáticas es con el objetivo de preservar la confidencialidad de la información de los distintos recursos, tanto para estudiantes como administrativos.

De tal manera para conservar dicha preservación y un buen control de acceso se recomienda:

1. **Creación de Usuarios**

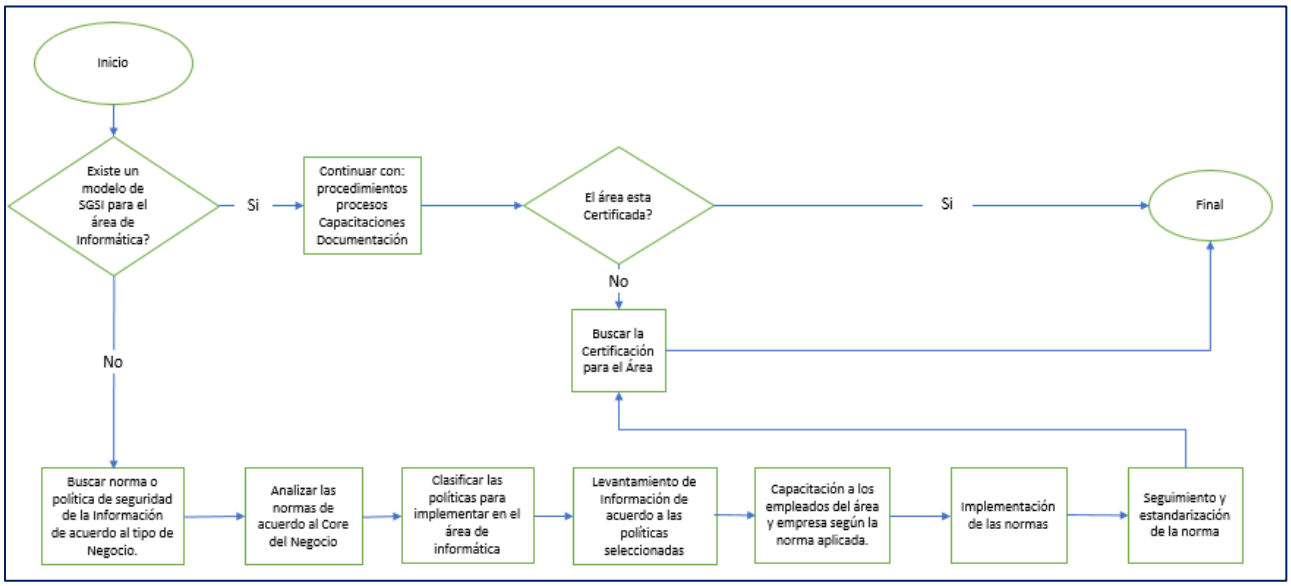
- Cada uno de los lideres o áreas responsables de los procesos haya autorizado a los administrativos o estudiantes a los diferentes sistemas de información de la entidad
- Los datos de acceso a la información deberán estar compuesto por un nombre de usuario y contraseña para cada uno de los usuarios ya sean administrativos o estudiantes de la institución deben ser únicos e intransferibles
- El funcionario o área responsable de la seguridad de la información deberá realizar revisiones de privilegios de acceso a los diferentes sistemas de información manteniendo los registros de las revisiones y hallazgos

2. **Administración de contraseñas de usuario**

- Todo usuario relacionado con acceso a un sistema de información de la institución ya sea administrativo o estudiante deberá cambiar su contraseña con una frecuencia recomendada a 6 meses.
- Todo sistema de información debería bloquear de manera temporal a los usuarios después de 5 intentos fallidos de autenticación.
- Determinar para contraseñas seguras a cada uno de los usuarios cumplir un mínimo de 8 caracteres incluyendo números, letras mayúsculas y en su posibilidad caracteres especiales.
- Establecer comunicado a todo usuario relacionado con acceso a la información en caso de cualquier incidente de inseguridad relacionado con sus contraseñas, bien sea por robo o indicio de perdida de confidencialidad a quien se debe notificar o que hacer.

Al aplicar la metodología anterior y realizando el ejercicio para conocer sobre la existencia de las políticas de seguridad de la información sobre estos tres Item (Seguridad de los recursos humanos, Gestión de activos de información, Control de accesos) en la Universidad los Libertadores, y aclarando los interrogantes de ¿Dónde estamos? y realizando el recorrido para sugerir con este articulo la pregunta ¿Dónde queremos estar?, entregamos en un diagrama de flujo la forma para identificar y aplicar las políticas de seguridad de la información con relación a las normas establecidas y de apoyo en las organizaciones como es la ISO 27001-2013.

Gráfica 7. Diagrama de Flujo_ Implementación de las Normas ISO 27001-2013



Fuente 9: El Autor

CONCLUSIONES

Entendiendo que cada día que pasa los avances a nivel de tecnología y comunicaciones son muy importantes, novedosos y fáciles de adquirir, también debemos tener claro que nos exponemos a mayores riesgos y amenazas a nivel de aplicaciones y programas, por este motivo toda empresa sin importar su Core de negocio y toda persona que incluya en su actividad diaria elementos de comunicación y almacenamiento de información como computadores y teléfonos inteligentes, debe protegerse de los posibles ataques que puede recibir por parte de un ciberdelincuente.

De igual manera como se cuidan y vigilan los activos de las empresas, entre estos la información, se debe mantener políticas o reglas claras y precisas para un mejor control y protección de la misma.

Es así como basándonos en los actuales procedimientos que tiene implementados la Universidad los libertadores en temas de seguridad de la información en el área de tecnología, y tomando como referencia 3 políticas (Gestión de Activos de la Información, Control de acceso y Seguridad de los Recursos Humanos) realizamos las recomendaciones que se describen en este documento, soportándonos en la información del procedimiento actual y de acuerdo a la ISO 27001-2013 entregando propuestas de valor que de ser apropiadas en la institución generan valor al área mencionada.

El documento lo trabajamos a nivel de recomendaciones a estas tres Políticas (Seguridad de los recursos humanos, Gestión de activos de información, y Control de accesos), de acuerdo a la norma ISO 27001-2013.

Nuestra entrega permite realizar un aporte a lo ya existente en la universidad, y desearles una mejora en todo o parte del proceso con las propuestas registradas.

REFERENCIAS

Banco santander. (12 de Septiembre de 2022). *Banco Santander*. Obtenido de https://www.bancosantander.es/glosario/disponibilidad-informatica#:~:text=Centr%C3%A1ndonos%20en%20el%20campo%20de,lo%20necesitan%20para%20desenvolver%20sus

Banco Santander. (12 de Septiembre de 2022). *Banco Santander*. Obtenido de https://www.bancosantander.es/glosario/integridad-seguridad-online#:~:text=Este%20t%C3%A9rmino%2C%20en%20seguridad%20inform%C3%A1tica,modificaci%C3%B3n%20no%20autorizada%20de%20esta.

César Wilfrido Astudillo-García, A. E.-D. (2019). *Políticas de gestión de seguridad de la información, fundamentadas en la norma.* Cuenca - Ecuador.

Fundacion Universitaria los Libertadores. (01 de Diciembre de 2017). Política Institucional de Seguridad de la Informacion. Bogota, Colombia.

GONZÁLEZ, A. C. (2013). *POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIVERSIDAD.* Bogota D.C.

https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf. (s.f.).

Icontec Internacional. (11 de Diciembre de 2013). NORMA TÉCNICA NTC-ISO-IEC.

Mintic. (01 de Noviembre de 2022). *Mintic*. Obtenido de Mintic: https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

TuDashboard. (20 de Octubre de 2021). *TuDashboard*. Obtenido de TuDashboard: https://tudashboard.com/analisis-gap/

Yuri Xiomara Becerra Rozo, R. D. (2022). *Políticas de Seguridad de la Información para la Universidad la Gran Colombia.* Bogotá.