MUST UNIVERSITY
MASTER OF SCIENCE IN BUSINESS ADMINISTRATION

RONNY JAVIER ORRALA VERA

IMPLEMENTACIÓN DE BUENAS PRÁCTICAS DE SEGURIDAD INFORMÁTICA EN EL LABORATORIO TEXCUMAR S.A. DE SANTA ELENA – ECUADOR.

FLORIDA – USA
2025

RONNY JAVIER ORRALA VERA

IMPLEMENTACIÓN DE BUENAS PRÁCTICAS DE SEGURIDAD INFORMÁTICA EN EL LABORATORIO TEXCUMAR S.A. DE SANTA ELENA – ECUADOR.

Trabajo de Conclusión Final presentado como requisito parcial para la obtención del título de MAESTRÍA en el Curso de MASTER OF SCIENCE IN BUSINESS ADMINISTRATION de MUST UNIVERSITY – Florida USA.

Orientador: Prof. Dr. Douglas Antonio Zelaya

FLORIDA – USA
2025

LISTA DE TABLAS

Tabla 1. Personal Texcumar. 16
Tabla 2. Tabulación de la Pregunta de Género 18
Tabla 3. Tabulación de la Pregunta de Edad 18
Tabla 4. Tabulación de la Pregunta de Años de Trabajo 19
Tabla 5. Tabulación de la Pregunta de Área de Trabajo 20
Tabla 6. Tabulación de la Pregunta #1 21
Tabla 7. Tabulación de la Pregunta #2 21
Tabla 8. Tabulación de la Pregunta #3 22
Tabla 9. Tabulación de la Pregunta #4 23
Tabla 10. Tabulación de la Pregunta #5 24
Tabla 11. Tabulación de la Pregunta #6 25
Tabla 12. Tabulación de la Pregunta #7 26
Tabla 13. Tabulación de la Pregunta #8 26
Tabla 14. Políticas del Sistema de Gestión de la Seguridad de la Información (SGSI). 37

LISTA DE FIGURAS

Figura 1. Porcentajes de Madurez Digital de las Empresas en el Ecuador 13
Figura 2. Estructura Organizacional Texcumar SA..... 14
Figura 3. Gráfico de Genero..... 18
Figura 4. Gráfico de Edad..... 19
Figura 5. Gráfico Años de Trabajo..... 19
Figura 6. Gráfico Área de Trabajo..... 20
Figura 7. Gráfico de la Pregunta #1..... 21
Figura 8. Gráfico de la Pregunta #2..... 22
Figura 9. Gráfico de la Pregunta #3..... 22
Figura 10. Gráfico de la Pregunta #4..... 23
Figura 11. Gráfico de la Pregunta #5..... 24
Figura 12. Gráfico de la Pregunta #6..... 25
Figura 13. Gráfico de la Pregunta #7..... 26
Figura 14. Gráfico de la Pregunta #8..... 27

RESUMEN

La presente investigación, aborda la implementación de buenas prácticas de seguridad informática en el laboratorio Texcumar S.A, ubicado en Santa Elena, Ecuador. La creciente dependencia de los sistemas tecnológicos en las operaciones empresariales ha incrementado la vulnerabilidad frente a filtración de información confidencial, lo que subraya la necesidad de contar con estrategias efectivas de protección. Este estudio se enfoca en identificar las principales brechas de seguridad informática en la organización, proponer soluciones basadas en normativas estructuradas y evaluar su impacto en la mejora de la seguridad y la continuidad del negocio.

La metodología utilizada en este estudio es cuantitativa por lo que se utilizó una encuesta como instrumento de recolección para conocer e identificar si existen procesos de seguridad aplicados a la documentación de la empresa. Entre los resultados destacados, se identificaron fallas en la gestión de documentos, ausencia de políticas de protección de datos e información y debilidades en la capacitación del personal sobre ciberseguridad. Las recomendaciones incluyen la adopción de medidas como manejar solo un tipo de archivo, aumentar niveles de accesos, aplicación estricta del Sistema de Gestión de la Seguridad de la Información (SGSI).

Los hallazgos revelan que la aplicación de buenas prácticas fortalece la resiliencia de la infraestructura tecnológica y disminuye el riesgo de incidentes informáticos. Este estudio contribuye no solo a la mejora del laboratorio Texcumar S.A., sino también a sentar un precedente para otras organizaciones locales que busquen optimizar su seguridad informática en un entorno cada vez más digitalizado.

Palabras clave: Seguridad informática. Buenas prácticas. Ciberseguridad.

ABSTRACT

This research addresses the implementation of good computer security practices in the TEXCUMAR S.A laboratory, located in Santa Elena, Ecuador. The increasing dependence on technological systems in business operations has increased vulnerability to confidential information leaks, underscoring the need for effective protection strategies. This study focuses on identifying the main computer security gaps in the organization, proposing solutions based on structured regulations and evaluating their impact on improving security and business continuity.

The methodology used in this study is quantitative, so a survey was used as a collection instrument to know and identify whether there are security processes applied to the company's documentation. Among the highlighted results, failures in document management, absence of data and information protection policies, and weaknesses in staff training on cybersecurity were identified. The recommendations include the adoption of measures such as managing only one type of file, increasing access levels, and strict application of the Information Security Management System (ISMS).

The findings reveal that the application of good practices strengthens the resilience of the technological infrastructure and reduces the risk of computer incidents. This study contributes not only to the improvement of the Texcumar S.A. laboratory, but also to setting a precedent for other local organizations seeking to optimize their computer security in an increasingly digitalized environment.

Key words: It security. Best practices. Cybersecurity.

IMPLEMENTACIÓN DE BUENAS PRÁCTICAS DE SEGURIDAD INFORMÁTICA EN EL LABORATORIO TEXCUMAR S.A. DE SANTA ELENA – ECUADOR.

Ronny Orrala Vera

SUMARIO

LISTA DE TABLAS II
LISTA DE FIGURAS III
RESUMEN IV
ABSTRACT V
SUMARIO VI
1 INTRODUCCIÓN 8
2. MARCO CONTEXTUAL Y MARCO TEÓRICO 9
2.1 Marco Contextual 9
2.1.1 Rasgos históricos 9
2.2 Marco Teórico 10
2.2.1 Ciberseguridad. 10
2.2.2 Buenas prácticas de seguridad de la información. 11
2.2.3 Prácticas de seguridad. 11
2.2.4 Ciberseguridad en Ecuador 12
2.2.5 Estructura organizacional de Texcumar SA. 13
3. DISEÑO METODOLÓGICO 14
3.1 Enfoque 15
3.2 Alcance 15
3.3 Diseño de la Investigación. 15
3.4 Participantes 16
3.4.1 Población. 16
3.4.2 Muestra 16
3.5 Método de Muestreo 16
3.5.1 Muestreo no probabilístico intencional o por juicio 16
3.6 Instrumentos. 17
3.7 Procedimiento Para la Recolección y Análisis de Datos. 17

4. ANÁLISIS Y RESULTADOS 17
4.1 Tabulación e Interpretación de Resultados 18
5. PROPUESTA DE LA IMPLEMENTACIÓN DE MEDIDAS DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN. 27
5.1 Tema 27
5.1.1 Objetivos 27
5.2 Descripción de la Propuesta 28
5.3 Norma de la Seguridad de Información *Web* 29
5.4 Políticas de Seguridad del Sistema 29
5.5 Análisis de Riesgos 30
5.6 Análisis de Factibilidad 31
5.6.1 Factibilidad técnica 31
5.6.2 Factibilidad operativa 31
5.6.3 Factibilidad económica 32
5.7 Desarrollo de la Propuesta. 32
6. CONCLUSIONES Y RECOMENDACIONES 39
6.1 Conclusiones 39
6.2 Recomendaciones 39
6.3 Consideraciones Finales 40
7. REFERENCIAS BIBLIOGRÁFICAS 41
8. ANEXOS 42

1 INTRODUCCIÓN

El presente estudio se justifica por la creciente vulnerabilidad de las empresas en Ecuador frente al robo de información confidencial. A menudo, las instituciones no cuentan con los recursos financieros ni el personal capacitado para implementar una infraestructura robusta de seguridad, lo que las convierte en objetivos atractivos para los delincuentes cibernéticos. En el caso de Texcumar S.A., la adopción de un enfoque estructurado en la gestión de información es esencial para mitigar riesgos y proteger sus sistemas y datos. Por lo tanto, resulta urgente estudiar, documentar e implementar estrategias que protejan a este tipo de organizaciones. Este proyecto busca llenar ese vacío, proporcionando un marco integral de medidas preventivas y reactivas ante potenciales incidentes.

La falta de medidas efectivas de ciberseguridad en el Laboratorio Texcumar S.A. ha aumentado la vulnerabilidad de documentos. Aunque la organización utiliza herramientas tecnológicas, no cuenta con un sistema de seguridad de datos que cumpla con proteger información, lo que pone en riesgo la confidencialidad, integridad y disponibilidad de sus activos digitales. Por consiguiente, esta investigación busca responder a la siguiente pregunta:

¿Es factible que la implementación de buenas prácticas de seguridad informática reduzca los riesgos cibernéticos en el Laboratorio Texcumar S.A. y asegurar la protección de sus activos digitales?

El objetivo del presente estudio es implementar procedimientos de buenas prácticas de ciberseguridad en el laboratorio Texcumar S.A. conociendo que la seguridad de los documentos es uno de los aspectos más importantes en toda empresa. Implementar una política de seguridad de documentos puede ser un proceso que requiere muchos recursos, pero se buscará la mejor alternativa para darle solución al problema principalmente la piratería de información.

Este estudio consta de partes fundamentales como la metodología que a través de un estudio descriptivo busca identificar los requisitos de un sistema de seguridad, desarrollar un esquema estructural de funcionamiento de la base de datos y diseñar una propuesta dinámica de buenas prácticas de gestión de documentos, también se encuentra estructurada por un enfoque de observación realizada en el laboratorio Texcumar, para constatar la gestión de la seguridad de los documentos que se utiliza actualmente, en este apartado se detalla la principal necesidad de desarrollo de la investigación. También consta del marco teórico, metodología, discusión de resultados, propuesta, conclusiones, recomendaciones y consideraciones finales.

El tratamiento de documentos planificados y eficientes pueden ayudar significativamente los procesos de producción y comercialización. El impacto del presente estudio mejorará la organización de la documentación y el respaldo local del laboratorio. Es importante implementar buenas prácticas de seguridad porque los archivos pueden contener datos confidenciales, como fórmulas de productos o datos personales que es necesario proteger de las vulnerabilidades de la red.

2. MARCO CONTEXTUAL Y MARCO TEÓRICO

2.1 Marco Contextual

2.1.1 Rasgos históricos

Existe un estudio realizado por Borky & Bradley, (2019), quien que se refiere a la "Protección de la información con ciberseguridad", como los sistemas actuales que se enfrentan a la amenaza de la información y el arquitecto del sistema que debe tener la capacidad de integrar medidas de seguridad características y funciones como elementos que garanticen la protección del sistema. Texcumar maneja información en los sistemas con un gran número de usuarios que pueden ser sensibles a ataques.

El autor Michener, (2016), con el tema “reglas simples para crear un buen plan de gestión de datos”, determina reglas simples para garantizar que los datos estén seguros y se puedan compartir. El presente estudio tiene como objetivo desarrollar métodos y enfoques estándar para gestionar información.

Langer, (2017), en su libro “Problemas de ciberseguridad en la tecnología de la información”, explica que se deben implementar medidas para garantizar la disponibilidad y veracidad de los datos. Generalmente a los correos de los trabajadores de Texcumar llegan mensajes cuyo objetivo es vulnerar información personal y laboral y estos ataques se activan simplemente abriendo links adjuntos.

Gliklich, Dreyer, & Leavy, (2016), en “Gestión de datos y garantía de calidad de respaldo de información”, determina los procedimientos de recopilación de datos y los principios de garantía de calidad para los registros. La gestión de información en la empresa Texcumar debería recopilar, almacenar y monitorear los datos del registro, para determinar la importancia de la información para su registro.

2.2 Marco Teórico

2.2.1 Ciberseguridad.

La implementación de tecnología es una estrategia necesaria dado que apoyan la toma de decisiones (Buenrostro & Hernández, 2019).

Con la tecnología actual, las empresas como Texcumar enfrentan nuevos desafíos para ser competitivos. Los sistemas de comunicación y la seguridad informática son parte fundamental para el funcionamiento de los procesos del negocio.

Es así, que se encuentran integrados como soporte para el desarrollo de las actividades productivas que generan valor a una empresa u organización.

La seguridad de procesamiento de la información, soporta la ejecución de los diferentes procesos que se encuentran automatizados para cada una de las áreas del negocio. El uso ininterrumpido de los sistemas de información y comunicación aumentan la eficacia y eficiencia de las organizaciones (Pabón, 2018).

En el presente estudio se analizarán un conjunto de normas de ciberseguridad que buscan responder si será ¿factible que la implementación de buenas prácticas de seguridad informática reduzca los riesgos cibernéticos en el Laboratorio Texcumar S.A. y asegurar la protección de sus activos digitales? Esto basado en normas internacionales referidas a la seguridad de la información y seguridad informática. Estas prácticas incluyen técnicas y controles de mitigación para contrarrestar los efectos de los riesgos a la seguridad informática que afectan a la integridad, disponibilidad y confidencialidad de la información.

2.2.2 Buenas prácticas de seguridad de la información.

Las buenas prácticas de seguridad de la información, representan un pilar fundamental en la protección de datos por lo que es necesario identificar definir e implantar prácticas necesarias para eliminar potenciales amenazas; a continuación, serán citadas.

2.2.3 Prácticas de seguridad.

La vulneración a la seguridad informática es necesaria en estos días. Es muy necesario manejar información y recursos para protegerse contra estas complejas y crecientes amenazas a la seguridad informática y mantenerse seguro en línea (Schattner, 2017). Algunas medidas preventivas que puede tomar incluyen:

- Analizar los medios de seguridad informática que utiliza el personal para el tratamiento de documentos en el laboratorio.

- Conocer cuáles son los departamentos que manejan día a día información confidencial para el proceso de producción del laboratorio.
- Identificar que sistemas informáticos utilizan actualmente para el tratamiento de documentos el personal del laboratorio.
- Instalación de *software* antivirus y de seguridad confiable y confiable.
- Activar su *firewall*, porque un *firewall* actúa como un guardia de seguridad entre Internet y su red de área local.
- Manténgase actualizado con el *software* y las noticias más recientes sobre sus dispositivos y realice actualizaciones de *software* tan pronto como estén disponibles.
- Evite hacer clic en los archivos adjuntos de correo electrónico a menos que conozca la fuente.
- Cambie las contraseñas con regularidad, utilizando una combinación única de números, letras y tipos de mayúsculas.
- Utilice Internet con precaución e ignore las ventanas emergentes y las descargas automáticas mientras navega.
- Tomarse el tiempo para investigar los aspectos básicos de la seguridad informática y educarse sobre la evolución de las ciberamenazas.
- Realice escaneos diarios completos del sistema y cree un programa periódico de respaldo del sistema para garantizar que sus datos sean recuperables en caso de que algo le suceda a su computadora.

2.2.4 Ciberseguridad en Ecuador

Ecuador ha adoptado la iniciativa del Banco Interamericano de Desarrollo para crear medidas de ciberseguridad que consiste en realizar un chequeo a los niveles de madures digital,

esta herramienta sirve de base para mejorar la gestión de seguridad digital de cada empresa además de medir y comparar los avances a lo largo del tiempo.

A continuación, se presentará un gráfico de un estudio aplicado a 617 empresas en donde se evidenció que la madurez digital tiene niveles deficientes (Reporte Chequeo Digital Ecuador, 2021).

Figura 1. Porcentajes de Madurez Digital de las Empresas en el Ecuador



Fuente: (Reporte Chequeo Digital Ecuador, 2021).

2.2.5 Estructura organizacional de Texcumar SA.

La estructura organizacional de Texcumar refleja el compromiso de la empresa por lograr una operación eficiente y un entorno de trabajo colaborativo que fomenta la innovación, el crecimiento y la calidad. A través de una organización jerárquica bien definida, Texcumar ha logrado establecer claras responsabilidades y una comunicación fluida entre los diferentes niveles y áreas.

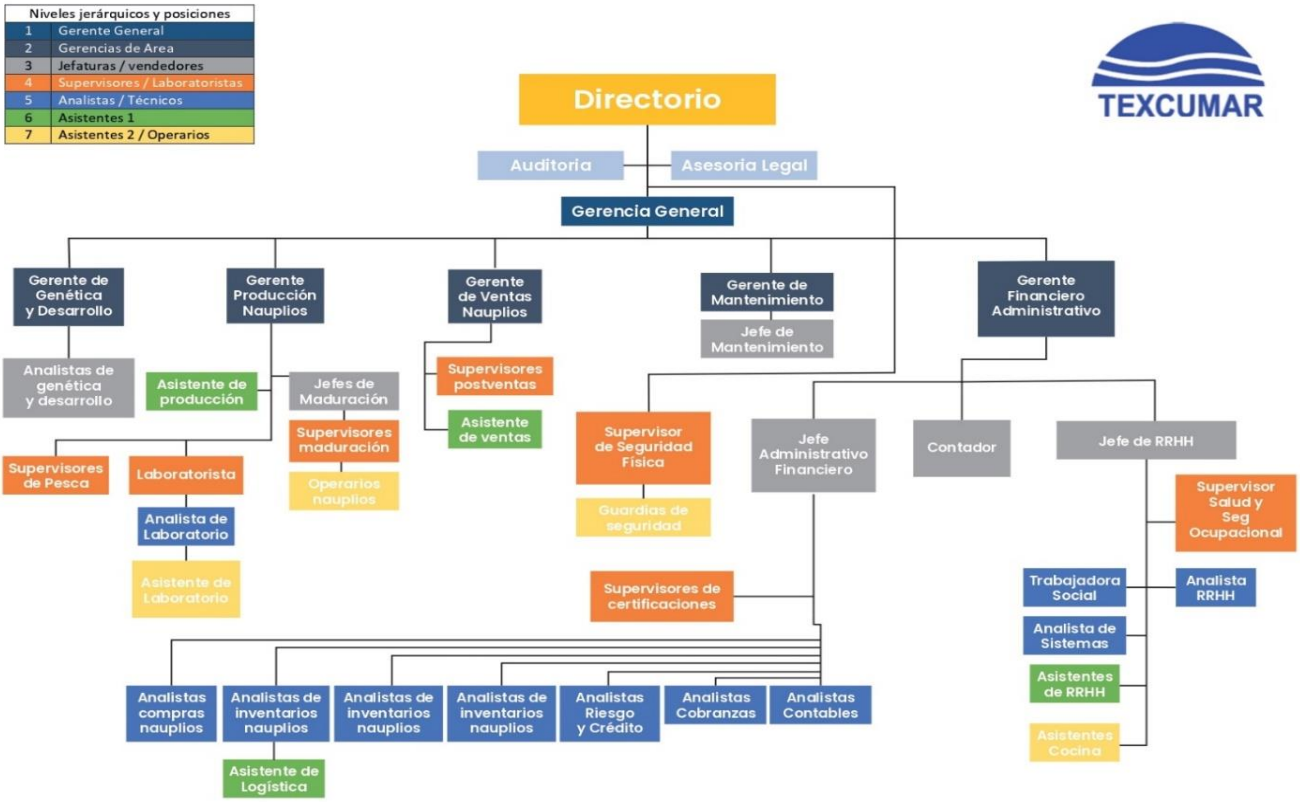
Cada departamento de Texcumar juega un papel crucial en el cumplimiento de sus objetivos estratégicos, desde la dirección general hasta las áreas operativas.

Esta estructura permite a la empresa mantener un enfoque centrado en el cliente, optimizando sus recursos y adaptándose de manera ágil a las necesidades del mercado.

Los accionistas juegan un papel crucial en la toma de decisiones y en la dirección futura de la compañía, destacando su participación y relevancia dentro del capital social.

La empresa Texcumar está conformada por un solo grupo de accionistas que es la sociedad Texcumar-Holding S.A.S. que es el socio único y principal de la compañía que está conformado por tres personas quien constituyen su capital social que es de $752,679.00. al cierre del año 2023.

Figura 2. Estructura Organizacional Texcumar SA



Fuente: Empresa Texcumar SA

3. DISEÑO METODOLÓGICO

El autor (Hernández Sampiere, 2014), indica en su Libro de Metodología de la Investigación que: “El sistema alude, en ese punto, a la hipótesis de las estrategias utilizadas en la exploración lógica y los procedimientos identificados con estas técnicas. En el debate intelectual sobre las diversas posturas en la metodología de la investigación, surge actualmente un fuerte ímpetu por respaldar y dar validez a aquellas orientadas hacia los aspectos cualitativos”

A continuación, se presenta la investigación a la institución Texcumar, para explicar las herramientas utilizadas para la recolección de datos.

3.1 Enfoque

El enfoque que tiene este estudio es cuantitativo debido a que la técnica de recolección de datos será por medio de una encuesta de evaluación al personal de las áreas de bodega, bacteriología, producción, genética y administración, las cuales sirvieron de apoyo para comprender los factores que influyen en la gestión de datos de la empresa Texcumar S.A. por medio de esto se analizará la eficiencia de las decisiones tomadas por los responsables de la seguridad de la información.

3.2 Alcance

La investigación descriptiva se dirige a describir el comportamiento de elementos variables o meramente identificar tipos (Curá, 2014, p. 105).

El alcance del presente estudio fue descriptivo; este tipo de investigación detalla aspectos fundamentales y los procedimientos de seguridad de la información de la empresa Texcumar S.A. a través de distintos indicadores que se utilizaron en esta investigación permitiendo conocer la situación actual de los procesos que se ejecutan en la institución.

3.3 Diseño de la Investigación.

El presente estudio es de carácter no experimental, ya que la investigación a la empresa Texcumar se realizó sin manipular intencionalmente los hallazgos encontrados.

3.4 Participantes

3.4.1 Población.

La población total involucrada fueron los trabajadores de la empresa Texcumar S.A. que corresponde a 324.

3.4.2 Muestra.

La muestra para ejecutar la encuesta son 52 trabajadores que son los que pertenecen a áreas que manejan día a día información confidencial para el proceso de producción de la empresa.

Tabla 1. Personal Texcumar.

Trabajadores	
Concepto	Cantidad
Bodega	4
Bacteriología	2
Producción	15
Genética	5
Administración	26
Total	52

Elaborada por el autor.

3.5 Método de Muestreo

3.5.1 Muestreo no probabilístico intencional o por juicio

En la empresa Texcumar actualmente trabajan 324 trabajadores la cual solo se aplicará la encuesta a 52 trabajadores que son los que manejan información confidencial según el criterio del investigador.

3.6 Instrumentos.

El instrumento fue una encuesta que inicia con preguntas personales sobre cada trabajador y continua con un banco de preguntas optativas utilizadas para recopilar información relacionadas con el objetivo de la presente investigación.

3.7 Procedimiento Para la Recolección y Análisis de Datos.

Para la recolección de datos se elaboró un cuestionario (ver anexo 2) y se analizó que todas las preguntas ayuden a obtener la información necesaria para alcanzar el objeto del estudio, para lo cual se desarrolló la matriz metodológica (ver anexo 1) de donde se obtuvo las dimensiones, indicadores y las respectivas preguntas; posteriormente se socializó y se obtuvo la autorización del gerente de la compañía para realizar la encuesta a los empleados objeto de la investigación en sus respectivos puestos de trabajo para obtener información relevante para el desarrollo del estudio (ver anexo 3), como siguiente paso se visitó en cada área de trabajo a los empleados y como consentimiento informado de los mismos firmaron su encuesta indicándoles que los datos obtenidos son exclusivos para el estudio formulado. Finalmente, los resultados obtenidos fueron tabulados los mismos que se evidencian a través de tablas y figuras que explican su interpretación y análisis general.

4. ANÁLISIS Y RESULTADOS

En esta sección se analizarán los datos obtenidos a través del cuestionario (ver anexo 2). Se visitó a las personas en su campo de acción, para poder tener información relevante para el desarrollo del estudio realizado, los resultados provenientes del presente articulo serán evidenciados a través de tablas y figuras que explican cada interpretación y análisis general.

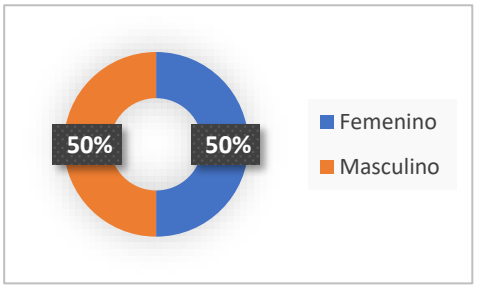
4.1 Tabulación e Interpretación de Resultados

Género

Tabla 2. Tabulación de la Pregunta de Género

Ítem	Respuesta	Porcentaje
Femenino	26	50%
Masculino	26	50%
Total General	52	100%

Figura 3. Gráfico de Genero



Fuente: Trabajadores de la empresa Texcumar S.A.
Elaborado por: Ronny Orrala.

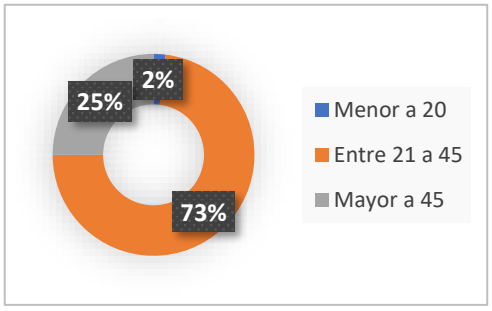
Interpretación: En la pregunta de género se encuesto a 26 mujeres que para el presente estudio representa el 50% y 26 hombres con el mismo porcentaje, la equidad de género se debe a que el área administrativa donde se maneja la mayor cantidad de información sensible está comprendida casi en su totalidad por mujeres mientras que la suma del resto de áreas encuestadas la integran hombres debido a que entre sus funciones también incluyen esfuerzo físico.

Edad

Tabla 3. Tabulación de la Pregunta de Edad

Ítem	Respuesta	Porcentaje
Menor a 20	1	2%
Entre 21 a 45	38	73%
Mayor a 45	13	25%
Total General	52	100%

Figura 4. Gráfico de Edad



Fuente: Trabajadores de la empresa Texcumar S.A.
Elaborado por: Ronny Orrala

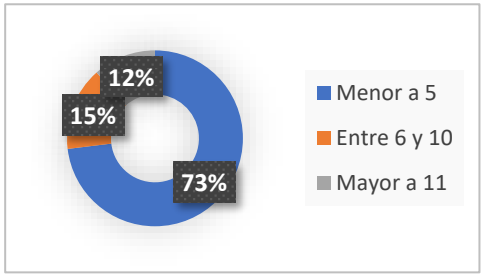
Interpretación: En la pregunta de edad predominan trabajadores de un rango de edad de entre 21 a 45 años con un total de 38 personas que para el estudio representa un 73%, seguido por 13 personas mayores de 45 años que ascienden a un 25% y finalmente 1 persona menor a 20 años con un 2%, el rango de 21 a 45 años de edad es el que la empresa considera que por experiencia conoce los procesos administrativos como los procesos de producción.

Años de Trabajo

Tabla 4. Tabulación de la Pregunta de Años de Trabajo

Ítem	Respuesta	Porcentaje
Menor a 5	38	73%
Entre 6 y 10	8	15%
Mayor a 11	6	12%
Total General	52	100%

Figura 5. Gráfico Años de Trabajo



Fuente: Trabajadores de la empresa Texcumar S.A.
Elaborado por: Ronny Orrala

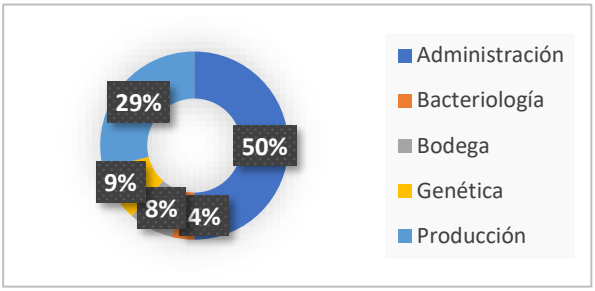
Interpretación: En la pregunta referente a los años que el personal encuestado trabaja en la institución predominan personal de un rango menor a 5 años con un total de 38 personas que para el estudio representa un 73%, seguido por 8 personas entre 6 y 10 años que ascienden a un 15% y finalmente 6 personas mayores a 11años con un 12%; el alto porcentaje de personas que han trabajo menos de 5 años incide negativamente a la custodia de datos sensibles de la empresa.

Área que Trabaja

Tabla 5. Tabulación de la Pregunta de Área de Trabajo

Ítem	Respuesta	Porcentaje
Administración	26	50%
Bacteriología	2	4%
Bodega	4	8%
Genética	5	10%
Producción	15	29%
Total General	52	100%

Figura 6. Gráfico Área de Trabajo



Fuente: Trabajadores de la empresa Texcumar S.A.
Elaborado por: Ronny Orrala

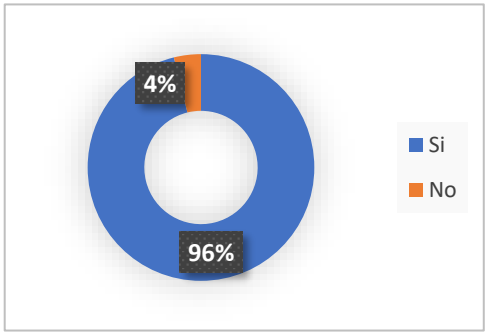
Interpretación: En la pregunta referente al área de trabajo del personal encuestado predominan administración con un total de 26 personas que para el estudio representa un 50%, seguido por 15 en producción que ascienden a un 29%, seguido por el área de genética con 5 trabajadores con un 10%, continua bodega con 4 personas con un 8% y finalmente 2 personas de bacteriología con un 4%; administración y producción son las áreas que manejan información sensible de la organización.

Pregunta 1: ¿La información que usted archiva puede hacerlo de forma digital?

Tabla 6. Tabulación de la Pregunta #1

Ítem	Respuesta	Porcentaje
Si	50	96%
No	2	4%
Total General	52	100%

Figura 7. Gráfico de la Pregunta #1



Fuente: Trabajadores de la empresa Texcumar S.A.
Elaborado por: Ronny Orrala

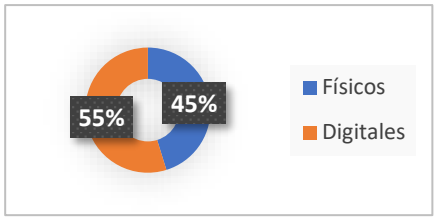
Interpretación: En la pregunta número 1 se manifiesta que 50 trabajadores pueden archivar la información que maneja de forma digital que representa un 96% y 2 personas con un 4% no pueden realizarlo; este resultado indica que la mayor parte de la información se digitaliza y que mejorando los procedimientos de seguridad informática se puede salvaguardar información confidencial de la organización.

Pregunta 2: ¿Qué medios de seguridad aplica para asegurar la documentación de su departamento?

Tabla 7. Tabulación de la Pregunta #2

Ítem	Respuesta	Porcentaje
Físicos	33	45%
Digitales	40	55%
Total General	73	100%

Figura 8. Gráfico de la Pregunta #2



Fuente: Trabajadores de la empresa Texcumar S.A.
Elaborado por: Ronny Orrala.

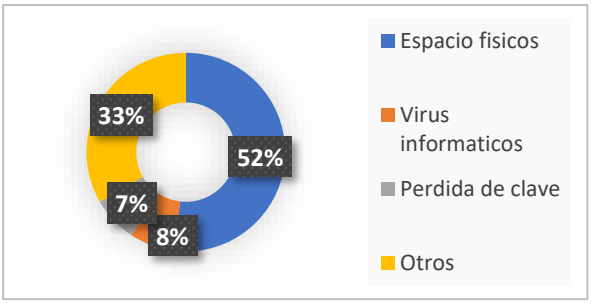
Interpretación: En la pregunta número 2 a pesar que la encuesta estaba diseñada para que las personas contestaran físicos o digitales existieron trabajadores que utilizaban las dos opciones y a su vez sugirieron el uso de las mismas, una vez aclarada esta novedad se puede manifestar que 40 personas utilizan medios de seguridad digitales lo que representa un 55% y 33 personas medios físicos que asciende a un 45%; entre los medios físicos que se utilizan se mencionaron memorias USB personales las cuales pueden ser utilizadas para sacar información sin autorización de la organización.

Pregunta 3: ¿Indique los problemas que se le ha presentado en relación al tratamiento de información?

Tabla 8. Tabulación de la Pregunta #3

Ítem	Respuesta	Porcentaje
Espacios físicos	28	52%
Virus Informáticos	4	7%
Perdida de clave	4	7%
Otros	18	33%
Total General	54	100%

Figura 9. Gráfico de la Pregunta #3



Fuente: Trabajadores de la empresa Texcumar S.A.
Elaborado por: Ronny Orrala.

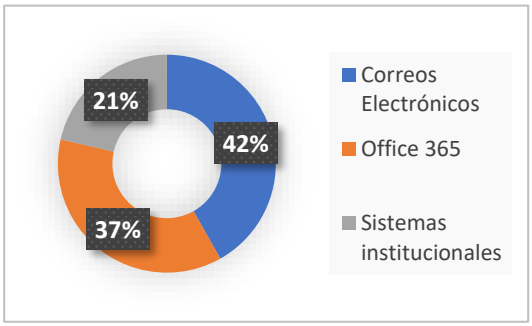
Interpretación: En la pregunta número 3 a pesar que la encuesta estaba diseñada para que las personas contestaran entre las opciones detalladas existieron trabajadores que utilizaban más de dos opciones, sugiriendo el uso de las mismas, una vez aclarada esta novedad se puede manifestar que 28 personas presentan problemas de espacio físico al momento del tratamiento de la información que representa un 52%, seguida por la opción otros con 18 personas que por la actualidad del país es la falta de energía eléctrica que representa un 33%, seguido por la opción perdida de clave con 4 personas con un 7% y finalmente virus informático con 4 personas con un 7%; la incertidumbre de no saber si podrán trabajar la jornada laboral completa con energía eléctrica obliga a los trabajadores respaldar información en dispositivos como USB los mismos que no presentan las garantías de seguridad necesarias para evitar filtración sensible de la organización.

Pregunta 4: ¿Indique que Sistemas Informáticos utiliza actualmente para el tratamiento de la información?

Tabla 9. Tabulación de la Pregunta #4

Ítem	Respuesta	Porcentaje
Correos Electrónicos	41	42%
Office 365	36	37%
Sistemas institucionales	21	21%
Total General	98	100%

Figura 10. Gráfico de la Pregunta #4



Fuente: Trabajadores de la empresa Texcumar S.A.
Elaborado por: Ronny Orrala.

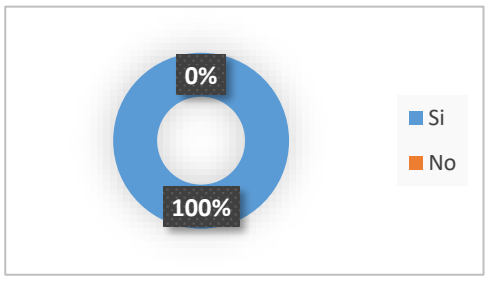
Interpretación: En la pregunta número 4 a pesar que la encuesta estaba diseñada para que las personas contestaran entre las opciones detalladas, existieron trabajadores que utilizaban más de dos opciones, y una vez aclarada esta novedad se puede manifestar que 41 personas utilizan correos electrónicos como sistemas informáticos para tratar información lo que representa un 42%, seguida por la opción Office 365 con 36 personas con un 37%, y finalmente sistemas institucionales con 21 personas con un 21%; esta pregunta demostró que casi toda la información se la respalda en correos electrónicos sean institucionales o personales por lo que las medidas de seguridad informática deben ser reforzadas.

Pregunta 5: ¿Considera que la institución requiere actualizar la estructura para la gestión de archivos y documentos?

Tabla 10. Tabulación de la Pregunta #5

Ítem	Respuesta	Porcentaje
Si	52	100%
No	0	0%
Total General	52	100%

Figura 11. Gráfico de la Pregunta #5



Fuente: Trabajadores de la empresa Texcumar S.A.
Elaborado por: Ronny Orrala

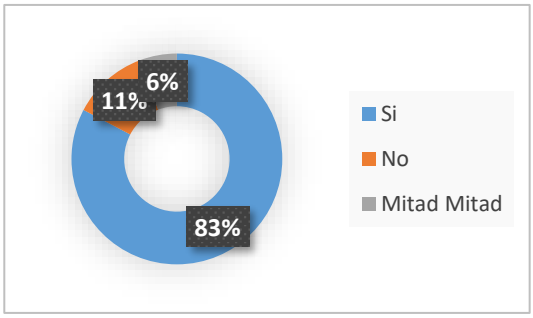
Interpretación: En la pregunta número 5 se manifiesta que 52 trabajadores consideran que la institución requiere actualizar la estructura para la gestión de archivos y documentos que representa el 100% de encuestados; es decir incluir nuevas medidas de seguridad para el trato de información confidencial.

Pregunta 6: ¿Cree usted que los documentos deberían almacenarse solo digitalmente para ahorrar espacio físico?

Tabla 11. Tabulación de la Pregunta #6

Ítem	Respuesta	Porcentaje
Si	43	83%
No	6	12%
Mitad mitad	3	6%
Total General	52	100%

Figura 12. Gráfico de la Pregunta #6



Fuente: Trabajadores de la empresa Texcumar S.A.
Elaborado por: Ronny Orrala

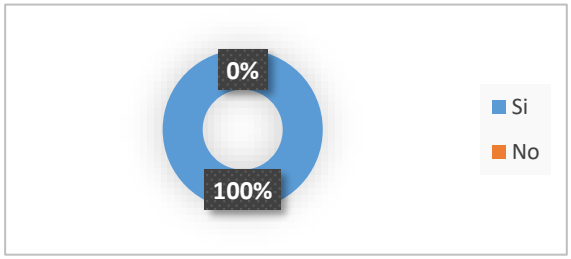
Interpretación: En la pregunta número 6 a pesar que la encuesta estaba diseñada para que las personas contestaran entre las opciones detalladas, existieron trabajadores que mencionaron que debería hacerse el almacenamiento mitad físico y mitad digital; una vez aclarada esta novedad se puede manifestar que 43 personas manifestaron que solo deberían almacenarse la información digitalmente para ahorrar espacio físico que representa un 83%, seguida de 6 personas que manifestaron que no solo físico con un 12% y finalmente con 3 personas que mencionaron que debería hacerse mitad con un 6%; los trabajadores manifestaron que digitalmente es más rápido ubicar cualquier tipo de documento.

Pregunta 7: ¿Estaría dispuesto a capacitarse en el manejo de buenas prácticas de seguridad informática?

Tabla 12. Tabulación de la Pregunta #7

Ítem	Respuesta	Porcentaje
Si	52	100%
No	0	0%
Total General	52	100%

Figura 13. Gráfico de la Pregunta #7



Fuente: Trabajadores de la empresa Texcumar S.A.
Elaborado por: Ronny Orrala

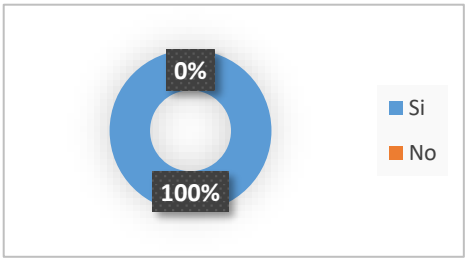
Interpretación: En la pregunta número 7 se manifiesta que 52 trabajadores estarían dispuestos a capacitarse en el manejo de buenas prácticas de seguridad informática que representa el 100% de los encuestados; como son normativas, procedimientos y guías para el manejo de información confidencial.

Pregunta 8: ¿Cree usted que la implementación de buenas prácticas de seguridad informática en el laboratorio ayude a proteger la integridad de la información?

Tabla 13. Tabulación de la Pregunta #8

Ítem	Respuesta	Porcentaje
Si	52	100%
No	0	0%
Total General	52	100%

Figura 14. Gráfico de la Pregunta #8



Fuente: Trabajadores de la empresa Texcumar S.A.
Elaborado por: Ronny Orrala

Interpretación: En la pregunta número 8 se manifiesta que 52 trabajadores creen que la implementación de buenas prácticas de seguridad informática en el laboratorio ayudará a proteger la integridad de la información que representa el 100% de los encuestados; la pregunta número 7 y 8 confirman que la implementación de normativas, procedimientos y guías para el manejo de información confidencial serán aceptadas y puestas en práctica por el personal de la organización.

5. PROPUESTA DE LA IMPLEMENTACIÓN DE MEDIDAS DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN.

5.1 Tema

Implementación de buenas prácticas de seguridad informática en el laboratorio TEXCUMAR S.A. de Santa Elena – Ecuador.

5.1.1 Objetivos

- Analizar que tipos de documentos se adapta mejor al sistema de buenas prácticas de seguridad informática

- Identificar niveles de acceso en el diseño de usuarios con *password* para cada una de las áreas que accedan al sistema.
- Definir las políticas del Sistema de Gestión de la Seguridad de la Información (SGSI).

5.2 Descripción de la Propuesta

En el laboratorio Texcumar S.A. de la provincia de Santa Elena, se genera una gran cantidad de documentación la cual toma tiempo al empleado en su administración y por lo tedioso del análisis de los datos que contienen, se desea implementar un sistema con buenas prácticas de seguridad informática.

En estas circunstancias, se plantearán medidas de seguridad que se adoptaría en el sistema con buenas prácticas. Dentro de las novedades identificadas en la investigación, existen pérdida de documentos, o que permanecen archivos sin saber si han sido actualizados o quién es el custodio de los mismos. Es decir, existe la inseguridad de la fiabilidad de la información que se maneja.

En esta propuesta se plantean medidas de seguridad como son políticas y procedimientos que permiten resguardar los sistemas informáticos de los peligros naturales y de la intromisión no autorizada a su base de datos.

El sistema con buenas prácticas de ciberseguridad será centralizado en su administración de archivos la cual recibirá, organizará, conservará y dispondrá los documentos de todas las unidades productoras de la institución a través de una red.

Dentro de las fases del planteamiento se seleccionó medidas adecuadas para el desarrollo y mejoramiento, entre las que se tiene: implementación de contraseñas seguras, eliminación de datos, mecanismos de defensa ante ataques externos y la seguridad física

5.3 Norma de la Seguridad de Información *Web*

La ISO 27001 es una norma internacional de Seguridad de la Información que asegura la confidencialidad e integridad de la información. Este estándar ha sido desarrollado por la Organización Internacional de Normalización (ISO: *"International Organization for Standardization*") y por la Comisión Electrotécnica Internacional (IEC: "*International Electrotechnical Commission"*) (ISO, 2018).

La norma define de manera independientemente los procesos de la organización como políticas, procedimientos y procesos; también cómo se planifica, implanta, verifica y controla un Sistema de Gestión de Seguridad de la Información, a partir de la realización de un análisis de riesgos y de la planificación e implantación de la respuesta a los mismos para su mitigación.

Se propone crear un sistema con buenas prácticas de ciberseguridad que permitirá la selección de los controles adecuados, mediante directrices como: acceso y derechos de uso; realizar evaluaciones periódicas de riesgos con el fin de verificar nuevas vulnerabilidades y controlarlas para garantizar las características y principios fundamentales de la ciberseguridad.

5.4 Políticas de Seguridad del Sistema

Las políticas de seguridad se plantearon con el fin de preservar, garantizar la integridad y disponibilidad de la información. Los documentos referentes a las políticas de seguridad contienen los procedimientos para cumplir las reglas y las responsabilidades en todos los niveles.

Las políticas de seguridad deben ser conocidas por todo el personal de la organización. En el manual de usuario que deben ser proporcionados por el desarrollador tienen que estar claramente establecidos: El objetivo, los responsables del cumplimiento y las medidas que se aplicarán en caso de incumplimiento.

Guías para el sistema con buenas prácticas de seguridad informática:

Administración de usuarios: normalizará el acceso a la información del personal

- **Copias de respaldo**: pasos a seguir para la recuperación de la información.
- **Tratamiento de la información**: establecerá los tipos de información que será manejada por personal autorizado.
- ***Software* legal:** definirá que *software* utilizará la institución.
- **Correo electrónico y servicio de Internet:** definirá la protección de la información mediante el uso de estos recursos.
- **Ambientes de procesamiento**: define los ambientes de procesamiento de información.
- **Seguridad en las comunicaciones**: protección de la información en los procesos de transmisión y recepción de datos.
- **Auditorías de los sistemas**: control de los procesos de seguridad en el sistema.
- **Protección física**: protección física de los equipos y las herramientas de procesamiento, almacenamiento y transmisión de datos.
- **Sanciones por incumplimientos**: medidas que se aplicarán por incumplimiento de la normativa.

5.5 Análisis de Riesgos

Se describirán las vulnerabilidades que requieren mayor atención en la implementación del sistema de buenas prácticas de seguridad informática

- **Fallos de Inyección**

Han existido correos no confiables enviados al personal que contenían *link* con comandos no confiables cuyo objetivo eran acceder a información sin autorización.

- **Perdida de Autenticación y Gestión de Sesiones**

Personal justifico la filtración de información alegando que habían accedido a su correo institucional sin autorización por lo que se debe proteger adecuadamente las credenciales de cuentas y los testigos de sesión.

- **Configuración defectuosa de seguridad**

Se evidencio la falta de mantenimiento y actualización del *software* lo que resultó en una defectuosa configuración de seguridad en los datos

- **Almacenamiento criptográfico inseguro**

Los correos electrónicos institucionales no utilizan funciones criptográficas para proteger datos y usuarios

- **Comunicaciones Inseguras**

Los correos fallan al autenticar y proteger la confidencialidad e integridad de tráfico de red sensible, esto ocurre debido a la utilización de algoritmos débiles, certificados expirados.

5.6 Análisis de Factibilidad

5.6.1 Factibilidad técnica

Es factible implementar un sistema de buenas prácticas de seguridad informática porque se cuenta con el talento humano y materiales para ejecutar normativas que actúen como estrategia de protección para la gestión de documentos que analice el nivel de seguridad y la amplitud de cualquier ataque externo que pueda vulnerar la información almacenada en la base de datos.

5.6.2 Factibilidad operativa

A nivel operacional, implementar un sistema de buenas prácticas de seguridad informática es factible porque el equipo a utilizar para ejecutar las normativas es parte de la

institución y se encuentra funcional, para ello ha sido necesario verificar la operatividad de un servidor *web*, un escáner y varios equipos de trabajo en donde se manipulará el sistema en la red para poder compartir información entre las estaciones de trabajo.

El personal para el manejo del sistema es:

- ✓ Programador.
- ✓ Secretaria del departamento de sistemas.
- ✓ Usuarios de los equipos conectados a la red.

5.6.3 Factibilidad económica

La implementación de un sistema de buenas prácticas de seguridad informática es económicamente viable, ya que la empresa cuenta con departamento correspondiente y el personal adecuado para llevar a cabo esta tarea. El analista de sistemas, responsable del área, se encargará de capacitar al personal en el uso de las buenas prácticas y de adaptar los equipos informáticos, tanto en términos de *hardware* como de *software*, según las especificaciones del manual para garantizar su correcto funcionamiento, además estos recursos y capacidades se encuentran disponibles debido a que dentro del presupuesto anual del Laboratorio Texcumar S.A. ya existen las partidas presupuestarias para la ejecución de este tipo de proyectos.

5.7 Desarrollo de la Propuesta.

Implementación de Buenas Prácticas de Seguridad Informática en el Laboratorio Texcumar S.A. de Santa Elena

Objetivo 1. Establecer los tipos de documentos que genera cada departamento en sus funciones diarias

Dentro de la documentación que se maneja en las áreas de bodega, bacteriología, producción, genética y administración, se encuentran:

- Documentos de *office* (docx, .xlsx y .pptx)
- Formato PDF

Si bien los departamentos que generan documentos transfieren la información al archivo central de acuerdo a los lineamientos establecidos por la institución, en este sistema es el archivo central quien reestablece y reconstruye el orden original de los archivos, respetando el principio de procedencia, a fines de categorización, ordenamiento y descripción.

Una etapa sensible del diseño es realizar el análisis de tipología documental de la organización, siendo base de la información recogida para la construcción de las herramientas de seguridad del Sistema los archivos en formatos digitales, entre otras.

Estos aspectos se identificaron en la encuesta que fue el instrumento principal, aportando con el análisis de las actividades de la organización, la identificación y documentación de cada función actividad y operación, la jerarquía entre ellas, así como el entorno normativo para proceder a implementar las presentes medidas de seguridad.

El análisis de tipología de los archivos, a más de dar las bases para el desarrollo del sistema de buenas prácticas de seguridad informática, permitirá distinguir en profundidad la trascendencia de los documentos más allá del contexto en que fue generado y realizar una propuesta de disposición documental con todas las normativas necesarias para el sistema.

Objetivo 2. Identificar niveles de acceso a través del diseño de usuarios con *password* para cada una de las áreas que accedan al sistema.

Los accesos son entregados de acuerdo a quién necesita saber, quién necesita usar y a cuánto acceso requieren. Los accesos son digitales y físicos basados en restricciones de permisos en las cuentas de usuario, así como limitaciones sobre quién puede acceder a ciertas direcciones físicas. Por ello, la política incluye:

Los requisitos del sistema con buenas prácticas de seguridad informática y su alineación con el esquema de clasificación de información en uso.

¿Quién solicita acceder?, conocer quién pide usar la información, todo ello con base en instrucciones establecidas para asignar el rol apropiado a cada usuario.

Administrar los derechos de acceso y derechos de acceso privilegiados, incluyendo las revisiones periódicas.

Controles de acceso reglamentados y que estén resguardados por procedimientos formales y responsabilidades definidas.

Acceso de usuarios

Cada usuario para ingresar al sistema debe tener definido un id y una clave, la primera pantalla que aparece al ejecutar el sistema consiste en la identificación del personal que ingresa. Así el programa solo deja acceder a aquellos que estén acreditados.

Cada empleado tiene un nivel de trabajo que es asignado por el administrador del sistema, no obstante, el administrador tendrá un acceso especial del sistema para ejecutar mantenimientos periódicos.

El rol de usuario se define según los niveles de trabajo los mismos que se encuentra en dos categorías:

El usuario administrador podrá realizar las siguientes tareas:

- Eliminar toda la base de datos.
- Acceso información de todos los usuarios.
- Ingresar información sensible.
- Cambiar información confidencial.
- Dar de baja información confidencial.
- Ejecutar auditoría general.

El usuario cliente solo podrá realizar las siguientes tares:

- Solicitar consultas de información.
- Ingresar o consultar información.
- Ver o eliminar información.

Control de *password.*

Esta opción está en el sistema para realizar el cambio de *password* y para la creación de nuevos usuarios, la asignación de los mismos en los diferentes puestos de trabajo es responsabilidad de usuarios de más nivel, se recomienda actualizar contraseñas periódicamente siendo requisito para esto combinar letras en mayúsculas, minúsculas y números.

Características de acceso al sistema

- **Confidencialidad** los datos sean manejados solo por personas autorizadas.
- **Integridad** su contenido solo puede ser modificado por usuarios autorizados
- **Disponibilidad**, información siempre lista para cubrir las necesidades de los usuarios
- **Control**, usuarios autorizados decidirán como y cuando manipular los datos.
- **Autenticidad,** datos válidos y usables.
- **Repudio**, un usuario que envió o recibió datos lo niegue

Objetivo 3. Definir las políticas del Sistema de Gestión de la Seguridad de la Información (SGSI).

Los datos del sistema con buenas prácticas de seguridad informática para el laboratorio Texcumar S.A. deben estar siempre protegidos.

Objetivos de seguridad de documentos

- ✓ Manejar los riesgos operacionales y estratégicos de la seguridad de datos en niveles aceptables para la institución.
- ✓ Proteger la confidencialidad de datos relacionada con los usuarios y con los planes de desarrollo.

- ✓ Almacenar la integridad de los registros de información.
- ✓ Cumplir con las especificaciones de disponibilidad requerida de los servicios *web* y redes internas
- ✓ Solucionar las necesidades de todas las partes interesadas.

Mecanismos de seguridad

El sistema con buenas prácticas de seguridad informática contiene los mecanismos de seguridad que ejecutan actividades específicas para la protección frente a ataques a la documentación. Pero existen mecanismos de seguridad principales son:

Cifrado, protege información con el uso de algoritmos matemáticos que transforman los datos originales en una secuencia de *bits* indescifrables para cualquier usuario no autorizado.

Control de acceso, mecanismo que solicita la autenticación y autorización para acceder a los recursos que se desee proteger.

Integridad de información**,** mecanismos utilizados para asegurar la integridad de los documentos o de un flujo de datos.

Intercambio de autenticación**,** asegura la identidad de usuario mediante un intercambio de información.

Tráfico de relleno, comprende en implantar *bits* en un flujo de datos para imposibilitar que tenga éxito un ataque por análisis de tráfico.

Control de encaminamiento, permite que la información siga unos definitivos enlaces y permite cambios en las rutas cuando se detecta que hay un problema de seguridad.

Seguridad perimetral, acepta o bloquea información recibida o enviada a un procesador ubicado fuera de la red local.

Políticas

El objetivo del sistema es proteger la información de la institución en contra de todas las amenazas y vulnerabilidades internas y externas.

Tabla 14. Políticas del Sistema de Gestión de la Seguridad de la Información (SGSI).

Políticas	Directrices	Definición
Respaldo y recuperación de datos	Los *Backups* se retendrán por un periodo establecido.	Seis meses se retendrán cada sistema, pasado este tiempo los *Backups* pueden eliminarse.
	La destrucción de los equipos de almacenamiento se realizará de manera segura.	Son los procedimientos formales para la destrucción de equipos que tengan datos confidenciales
	El acceso a los equipos de almacenamiento debe ser restringido.	Los equipos donde se almacenan los *Backups* no serán manipulados por personal sin autorización.
	Antes de hacer cambios se harán un *Backup*.	Es necesario hacer un *Backup* de los sistemas de información antes de cualquier cambio.
	Antes de actualizar tecnológica sobre las plataformas del sistema, se debe cargar la información a la nueva plataforma	Cuando se actualice tecnología en las plataformas del sistema se debe asegurar que la información que se encuentra en el sistema antiguo, sea trasferida al nuevo.
Estaciones de trabajo	Estaciones de trabajo	Las estaciones de trabajo de los usuarios estarán configuradas, para ser usadas exclusivamente para el desarrollo de las funciones de su cargo; se prohíbe el almacenamiento de información personal y su acceso será mediante el usuario y contraseña
	Dispositivos de almacenamiento externo.	Las entradas para dispositivos de almacenamiento externos estarán deshabilitadas en cada equipo, y únicamente para los usuarios que lo soliciten por escrito se les habilitara previo análisis de su requerimiento.
	Detección de *malware*	Este *software* protegerá al sistema operativo en tiempo real y de actualizarse de forma automática.
	Manipulación del *software* del sistema.	La configuración del *software* del sistema estará protegida en cada estación de trabajo.

	Servicio de navegación a internet.	El servicio de navegación en internet de los empleados desde estaciones de trabajo solo se autorizará para fines de trabajo y solo estará habilitado el acceso al correo institucional.
Protección contra el *Malware.*	Prohibido uso de *software* malicioso.	Prohibiese a los usuarios copiar, propagar o ejecutar sistemas tecnológicos con *software* malicioso
	Procedimientos de protección contra el malware.	Se les socializara un instructivo que guie sobre de las acciones a tomar, cuando se evidencia *malware* en el sistema.
	Herramientas *antimalware*	Servidor debe tener instalado configurado y actualizado la solución institucional de protección contra el *malware*.
	Empleados serán garantes de la configuración que se les entrega	Cuando se evidencie cualquier anomalía de la configuración, deberá ser reportado de manera inmediata al área de seguridad de la información.
Gestión de incidentes en la seguridad de datos	Compromiso de la gerencia	La gerencia hará cumplir la presente normatividad para la atención de estos incidentes en seguridad de la información
	Identificación de eventos	Personal debe tener la capacidad para determinar las causas de un posible incidente en seguridad de datos
	Comunicación de incidentes.	Los incidentes de seguridad de datos serán informados describiendo el evento presentado y se tratara con la mayor confidencialidad.
Gestión de red de datos	Inhabilitar puertos de red en desuso	Se deshabilitará servicios y puertos de red que no se requieren para el funcionamiento del sistema, al igual que las interfaces que no estén autorizadas
	Instalar equipos de red debe ser documentada.	Se deben mantener registro documentado que especifique la trazabilidad de la gestión de la red de datos.
	Dispositivo de *networking* deberán ser autorizado antes de conectarse a la red de datos	Los permisos de dispositivos que necesiten conectarse a la red de datos, se deben solicitar al administrador para su autorización.

	Transmisión de datos en redes públicas	La información confidencial durante su transmisión a través de las redes donde el acceso es abierto y/o sin restricción se debe desarrollar por medio de mecanismos de cifrado para garantizar la integridad de los datos

Fuente: Elaborado por el autor.

6. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Los tipos de archivos que se generan en las áreas de bodega, bacteriología, producción, genética y administración del laboratorio Texcumar S.A. son documentos de office (docx, .xlsx y .pptx) y formato PDF,

Se identificó niveles de acceso en el diseño de usuarios con *password* para cada una de las áreas que accedan al sistema basadas en políticas de seguridad que se establecerían en el desarrollo del sistema.

Se Definió las políticas del Sistema de Gestión de la Seguridad de la Información (SGSI). que garantizarán confidencialidad, disponibilidad e integridad en conjunto de la correcta funcionalidad de la gestión de información.

6.2 Recomendaciones

Solicitar subir al sistema un solo tipo de archivo el que sería en formato pdf, que por el tamaño de carga contribuirá a que el sistema no se cuelgue haciendo el mismo más seguro y factible.

Se debe hacer uso de todos los niveles de seguridad propuesta para la generación de los usuarios y *password.*

El desarrollador debe tomar en cuenta y aplicar las políticas del Sistema de Gestión de la Seguridad de la Información (SGSI) para garantizar el cumplimiento del objetivo de las medidas de seguridad.

6.3 Consideraciones Finales

Hay cambios sustantivos en la arquitectura institucional de la ciberseguridad del laboratorio a corto y mediano plazo y la tendencia es su manutención, con todos los problemas de atribución que la acompañen.

Texcumar debe actualizar la política de ciberseguridad en tiempos periódicos para ir a la par con los problemas de seguridad que enfrentará en el futuro.

Superar la fragmentación en su estructura institucional es fundamental para que las iniciativas de ciberseguridad en la empresa y en cooperación con empleados sean más coherentes.

Investigaciones futuras en el área de ciberseguridad, deben considerar y no estimar esfuerzos en ese sentido, como también las iniciativas de cooperación entre instituciones con la misma razón social en materia de ciberseguridad, así como la participación del sector privado en la construcción de un papel global más protagonista para las empresas.

7. REFERENCIAS BIBLIOGRÁFICAS

Borky, J. M., & Bradley, T. H. (2018). Protección de la información con ciberseguridad. Ingeniería de sistemas eficaz basada en modelos, 345–404. https://doi.org/10.1007/978-3-319-95669-5_10

Michener, W. K. (2016). Reglas simples para crear un buen plan de gestión de datos. *PLoS Computational Biology*, 11(10). https://doi.org/10.1371/journal.pcbi.1004525

Langer, S. G. (2017). Problemas de ciberseguridad en la tecnología de la información. *Journal of Digital Imaging*, 30(1), 117–125.

Gliklich, R., Dreyer, N., & Leavy, M. (2016). Gestión de datos y garantía de calidad de respaldo de información. En Registros para evaluar los resultados de los pacientes: una guía del usuario. Agencia para la Investigación y la Calidad.

Buenrostro, H. E., & Hernández, M. D. (2019). La incorporación de las TIC en las empresas. Factores de la brecha digital en las MIPYMES de Aguascalientes. Economía, teoría y práctica, 50, 101–124.

Pabón, F. O. (2018). Retos y tendencias de la ingeniería en tecnologías de la información y las comunicaciones (TIC) frente al desarrollo del sector productivo. Retos, 14, 39.

Schattner, P. (2017). *Guidelines for computer security in general practice. Journal of Health Informatics*, 15(2), 73–82. https://doi.org/10.14236/jhi.v15i2.645

Equipo editorial. (2021, 5 de agosto). Sistema de información. Concepto de. https://concepto.de/sistema-de-informacion/

Hernández Sampieri, R. (2014). Metodología de la investigación (6.ª ed.). México D.F.: McGraw-Hill Interamericana.

Curá, J. (2014). Metodología de la investigación. Revista Jurídica UCES.

8. ANEXOS

Anexo 1. Matriz Metodológica

Tema	Justificación	Objetivos	Pregunta	Enfoque, alcance y diseño	Variables	Dimensiones	Indicadores	Instrumento de recolección de datos	Preguntas	Población y Muestra	Resultados
IMPLEMENTACIÓN DE BUENAS PRÁCTICAS DE SEGURIDAD INFORMÁTICA EN EL LABORATORIO TEXCUMAR S.A.	Seguridad en la gestión de documentos	Identificar si existen procesos de seguridad aplicado a la documentación de la empresa Texcumar S. A	¿Qué beneficios adquirirá la empresa TEXCUMAR S.A. con la implementación de buenas prácticas para la seguridad de documentos?	Enfoque: Cuantitativo	Implementación de buenas prácticas de seguridad	Procesos de seguridad	Tipo de Información Medidas de seguridad Tipo de problemas	Encuesta	1, 2, 3,4	Población: La población total involucrada fueron los trabajadores de la empresa Texcumar SA	Nivel de aplicación de procesos de seguridad
		Desarrollar una normativa estructural para el sistema de buenas prácticas de seguridad		Alcance: Descriptivo		Normativa estructural	Actualización de estructura		5		Porcentaje de actualizar estructura
					Proteger la integridad de la documentación	Buenas prácticas de seguridad	Almacenamiento digital Capacitación		6, 7, 8	Muestra: La muestra para ejecutar la encuesta son 52 trabajadores.	Proteger la integridad de la información

		Diseñar una propuesta de buenas prácticas de seguridad para documentos en la empresa TEXCUMAR S.A.		Diseño: no experimental							

Anexo 2. Encuesta

Es importante mencionar que sus respuestas serán manejadas con total reserva, y el uso de la información es exclusivo para el estudio formulado.

Instrucciones: Por cada pregunta deberá elegir una opción marcando en el cuadro de su preferencia con una X.

Sexo: Femenino ☐ Masculino ☐

Edad: Menor a 20 ☐ Entre 21 y 45 ☐ Mayor de 45 ☐

Años de trabajo: Menor a 5 ☐ Entre 6 y 10 ☐ Mayor a 11 ☐

Área que trabaja: Administrativa ☐ Bacteriología ☐ Bodega ☐

Genética ☐ Producción ☐

1. ¿La información que usted archiva puede hacerlo de forma digital?

Si ☐ No ☐

2. ¿Qué medios de seguridad aplica para asegurar la documentación de su departamento?

Físicos ☐ Digitales ☐

3. ¿Indique los problemas que se le ha presentado en relación al tratamiento de información?

Espacio físico ☐ Virus informáticos ☐ Perdida de claves ☐ Otros_____

4. ¿Indique que Sistemas Informáticos utiliza actualmente para el tratamiento de la información?

Correos Electrónicos ☐ Office 365 ☐ Sistemas institucionales ☐

5. ¿Considera que la institución requiere actualizar la estructura para la gestión de archivos y documentos?

Si ☐ No ☐

6. ¿Cree usted que los documentos deberían almacenarse solo digitalmente para ahorrar espacio físico?

Si ☐ No ☐

7. ¿Estaría dispuesto a capacitarse en el manejo de buenas prácticas de seguridad informática?

Si ☐ No ☐

8. ¿Cree usted que la implementación de buenas prácticas de seguridad informática en el laboratorio ayude a proteger la integridad de la información?

Si ☐ No ☐

_____
Firma

Anexo 3. Listado de Personas Encuestadas de la Empresa Texcumar S.A.

No	Departamento/Área	Nombre del Trabajador
1	Administrativa	Aguayo Lindao Ingrid Annabelle
2	Administrativa	Albornoz Osorio Andrea Carina
3	Administrativa	Andrade Luque Sergio Eduardo
4	Administrativa	Arteaga Flores Carolay Analy
5	Administrativa	Baquerizo Orrala Lizzy Nicole
6	Genética	Beltrán Usho Emily Luisana
7	Genética	Borbor Del Pezo Jefferson Ronald
8	Producción	Borbor Domínguez Geovanny Juan
9	Administrativa	Carrera Lazo María Daniela
10	Administrativa	Chalen Rodríguez Rosa María
11	Producción	Conforme Pincay Pedro Eladio
12	Administrativa	Cordero Linzan Mayra Gabriela
13	Bacteriología	Córdova Lindao Grecia Analí
14	Genética	Cox Conforme Carlos Andrés
15	Producción	Cruz Méndez Rómulo Eduardo
16	Administrativa	De la Avendaño Priscila Noralma
17	Administrativa	García Gallegos Bernardo Xavier
18	Producción	Guerrero López Marcelo Héctor
19	Bodega	Holst Pérez Emil Efraín
20	Producción	Lino Laínez Líder Stalin

21	Administrativa	Lino Moran Melissa Elizabeth
22	Administrativa	Linzan Linzan Ana Teresa
23	Genética	Lopes Da Costa Rocha Joao Luis
24	Administrativa	López Laínez Lissette Alexandra
25	Administrativa	Malavé Laínez Jenny Del Roció
26	Producción	Marcillo Moreira Tulfo Gabriel
27	Bodega	Merejildo Rodríguez Oscar Eduardo
28	Administrativa	Montero Guambuguete Alex Darío
29	Producción	Muñoz Alejandro Darwin Andrés
30	Producción	Muñoz Reyes Jhon Homero
31	Administrativa	Panimboza Tigrero Jessica Nataly
32	Bodega	Pilay Reyes Rubén Arturo
33	Administrativa	Regalado Arreaga Olga Bella
34	Producción	Regalado Mora Jimmy Virgilio
35	Administrativa	Reyes Fiallos Adriana Carolina
36	Producción	Reyes Villamil Nelson Lenin
37	Administrativa	Salas Tigrero Ana Mariuxi
38	Administrativa	Salvador Moncayo Karen Tatiana
39	Bacteriología	Solís Rivera Alexandra Micaela
40	Producción	Suarez Izquierdo José Leonel
41	Producción	Suarez Orrala Jairo Javier
42	Producción	Taco Panchi Cesar Hernán
43	Administrativa	Tigrero Bravo Gardenia Estefanía
44	Producción	Tomalá Caiche Cristhian Celso
45	Administrativa	Toro Gonzabay María De Los Ángeles
46	Administrativa	Tumbaco Muñoz Henry Hugo
47	Administrativa	Velásquez García Jessica Indira
48	Administrativa	Verduga Regalado Rafael Ernesto
49	Producción	Villao Suarez Wilmer Alfredo
50	Bodega	Villavicencio Castro Frank Jhonny
51	Administrativa	Zambrano Maldonado Diana Estefanía
52	Genética	Zambrano Orrala Fernanda Lisbeth