UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO

TEMA:

PROPUESTA DE ENSEÑANZA DE CIBERSEGURIDAD PARA EJECUTIVOS CON LA FINALIDAD QUE TRANSFORMEN, LIDEREN Y APLIQUEN EN SUS EMPRESAS

AUTOR:

CARLOS JAVIER OROZCO BELLO

DIRECTOR:

JOSÉ LUIS AGUAYO MORALES

CUENCA – ECUADOR
2024

Autor:

Carlos Javier Orozco Bello
Licenciado en Computación.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
corozcob1@est.ups.edu.ec

Dirigido por:

José Luis Aguayo Morales
Ingeniero en Sistemas.
Magister en Sistemas Informáticos Educativos.
Magister en Redes de Comunicaciones.
Magister en Ciberseguridad.
jaguayo@est.ups.edu.ec

DEDICATORIA

Dedico este logro a mi amado hijo, quien, a pesar de la distancia, siempre ha sido mi inspiración de superación. Que la constancia y dedicación me recuerdan que no hay meta demasiado lejana si se enfrenta con determinación.

A mi querida madre, aunque ya no esté entre nosotros físicamente, sé que su espíritu sigue guiándome desde donde esté. Su amor incondicional y sus sabias palabras continúan siendo mi fuerza en cada paso que doy.

A mi padre ejemplar, cuyos consejos resonaron en mí desde mi infancia. Él me enseñó que el aprendizaje es un viaje sin fin, y su legado vive en cada logro que alcanzo.

A mis valientes hermanos, compañeros de vida. Su apoyo inquebrantable y su presencia constante han sido mi roca en los momentos más difíciles. Juntos, hemos superado desafíos y celebrado victorias, construyendo recuerdos que atesoro con cariño.

AGRADECIMIENTO

Quiero agradecer a mis profesores, especialmente a mi tutor José Luis Aguayo Morales, por su guía y apoyo constante. Agradezco a la Universidad Politécnica Salesiana por brindarme una educación de calidad.

Gracias también a mis compañeros de estudio por su colaboración y compañerismo. A mi familia, por su amor incondicional y apoyo constante.

Y finalmente, gracias a todos los que contribuyeron de alguna manera a este logro. Su presencia y apoyo han sido fundamentales en mi camino hacia el éxito.

Tabla de Contenido

Propuesta de enseñanza de ciberseguridad para ejecutivos con la finalidad que transformen, lideren y apliquen en sus empresas

Autor(es):

Carlos Javier Orozco Bello

Resumen

La ciberseguridad es fundamental para proteger datos y garantizar la continuidad operativa, en un mundo cada vez más orientado a lo digital y globalizado. La empresa estudiada, especializada en servicios de Cobranzas y Business Process Outsourcing (BPO), enfrenta desafíos en la administración de la seguridad de la información y salvaguardar la privacidad de los datos sensibles de sus clientes, agravados por regulaciones como lo es el COIP (Código Orgánico Integral Penal) y la Ley de Protección de Datos Personales en Ecuador.

A pesar de inversiones en seguridad, persisten riesgos de filtración de datos. La empresa ha creado el departamento de Riesgos y cuenta con la certificación ISO 27001, pero persiste una brecha de conocimiento en ciberseguridad entre los ejecutivos.

El objetivo de esta investigación es cerrar esta brecha mediante un programa de capacitación específico. La metodología aplicada se basa en el modelo ADDIE, combinando métodos cualitativos y cuantitativos. Se llevaron a cabo entrevistas y cuestionarios para recopilar información sobre la comprensión y necesidades de capacitación de los ejecutivos.

Los resultados indican una limitada comprensión de las amenazas cibernéticas previo al programa. Tras su implementación, se observa un notorio aumento en la comprensión y sensibilización acerca de la importancia de la ciberseguridad. Esto evidencia la eficacia del programa para fortalecer la postura de seguridad cibernética de la empresa. La capacitación cerró la brecha de conocimiento en ciberseguridad entre los ejecutivos, contribuyendo a resguardar la información confidencial de los clientes en un entorno empresarial digitalizado y sujeto a regulaciones.

Palabras claves:

Ciberseguridad, capacitación ejecutiva, regulaciones legales, cultura de seguridad.

ABSTRACT

In an increasingly digitized and globalized business environment, cybersecurity is paramount for protecting data and ensuring operational continuity. The studied company, specialized in Debt Collection and Business Process Outsourcing (BPO) services, faces challenges in managing information security and protecting sensitive customer data, exacerbated by regulations such as the Personal Data Protection Law and the Comprehensive Organic Penal Code (COIP) in Ecuador.

Despite investments in security, data leakage risks persist. The company has established the Risk department and holds ISO 27001 certification, yet a knowledge gap in cybersecurity among executives persists.

The aim of this research is to close this gap through a specific training program. The methodology applied is based on the ADDIE model, combining qualitative and quantitative methods. Interviews and questionnaires were conducted to gather information on executives' understanding and training needs.

Results show a limited understanding of cyber threats before the program. After its implementation, a significant increase in knowledge and awareness of the importance of cybersecurity is observed. This demonstrates the program's effectiveness in strengthening the company's cybersecurity posture. This training program closed the cybersecurity knowledge gap among executives, contributing to protecting sensitive customer data in a digitized and regulated business environment.

Keys Words:
Cybersecurity, executive training, legal regulations, security culture.

1. Introducción

En el panorama empresarial contemporáneo, la digitalización ha remodelado fundamentalmente la forma en que las organizaciones operan, interactúa y compiten. La expansión de la tecnología y la abundancia de datos han impulsado un cambio de paradigma, donde la información se ha convertido en el activo más valioso y, a su vez, en el objetivo principal de los ciberataques. En este contexto, la ciberseguridad emerge como un dominante estratégico para la protección de los datos empresariales y la sostenibilidad de las organizaciones en un entorno cada vez más amenazador y complejo.

En la empresa donde se realizó la investigación, es una compañía líder en servicios de Cobranzas y Business Process Outsourcing (BPO), se encuentra en la vanguardia de este escenario empresarial dinámico. Al proporcionar servicios a diversas empresas, maneja una gran cantidad de datos sensibles y personales de sus clientes, los cuales otorgan distintas empresas bancarias, cooperativas y aseguradoras que se encuentran operando en Ecuador. Sin embargo, esta posición privilegiada también la expone a riesgos significativos de ciberseguridad, que pueden comprometer la confidencialidad, integridad y disponibilidad de los datos, que en muchos de los casos son información que no pueden llegar a caer a manos de tercero, si esto ocurre las leyes que rigen en el país pueden actuar sobre la empresa o colaboradores que las infligen.

A pesar de las inversiones en tecnologías de seguridad y la implementación de medidas preventivas, la empresa enfrenta desafíos persistentes en la protección de datos. La existencia de regulaciones legales como la Ley Orgánica de Protección de Datos Personales y el Código Orgánico Integral Penal (COIP) en Ecuador, que establece sanciones por la divulgación y mal manejo de datos, subraya la importancia crítica de fortalecer la ciberseguridad en todas las organizaciones.

En la Ley de Protección de Datos, que se aprobó en mayo de 2021 y se encuentra en vigencia desde mayo del 2023, en el artículo 37 indica que la importancia de que los responsables o encargados del tratamiento de estos datos sigan el principio de seguridad. Esto implica considerar aspectos como la cantidad y tipo de datos, el nivel tecnológico, las mejores prácticas de seguridad y los costos involucrados. Acá enfatiza la necesidad de un proceso continuo de evaluación de las medidas implementadas para garantizar la eficacia y eficiencia en la protección de los datos. Se mencionan medidas específicas, como la anonimización o el cifrado de datos, así como la importancia de mantener la confidencialidad, integridad y disponibilidad de los sistemas y servicios de tratamiento de datos. Se sugiere el uso de estándares internacionales y códigos de conducta reconocidos para una gestión adecuada de riesgos y la protección de derechos y libertades. [1]. Donde la empresa está obligada a tomar medidas activas para proteger los datos personales que maneja, evaluar y mejorar constantemente su seguridad, y cumplir con estándares tanto nacionales como internacionales en materia de protección de datos.

Adicional, se encuentra el artículo 178 del Código Orgánico Integral Penal (COIP) que en resumen indica que cualquier individuo que sin el consentimiento o la autorización legal acceda, intercepte, examine, retenga, grabe, reproduzca, divulgue o publique datos personales u otra información privada de alguien, será sancionado con una pena de prisión de uno a tres años [2], interpretando, la empresa está obligada a respetar la privacidad y la confidencialidad de dichos datos.

La relevancia de esta investigación radica en que, a pesar de los crecientes riesgos cibernéticos, los cuales son intentos maliciosos de acceder o dañar un sistema de computadoras o redes, que pueden ocasionar robo de información personal [3], muchos ejecutivos carecen de un entendimiento profundo de las amenazas y las estrategias de ciberseguridad necesarias para proteger sus organizaciones. Esto puede resultar en decisiones estratégicas insuficientemente informadas y en una falta de liderazgo en la implementación de medidas de seguridad adecuadas. La brecha de conocimiento en ciberseguridad entre los técnicos y los ejecutivos puede

poner en peligro la continuidad operativa, la reputación y la confianza de los clientes.

En este contexto, la presente investigación se enfoca en un desafío clave: la brecha de conocimiento en ciberseguridad entre los ejecutivos y líderes empresariales de la empresa. Aunque la empresa ha implementado medidas de concientización, persiste una falta de comprensión profunda de las amenazas cibernéticas, leyes vigentes y las estrategias de seguridad necesarias para proteger la empresa y sus clientes.

Esta brecha de conocimiento plantea riesgos significativos, tanto para la empresa como para sus clientes. La falta de liderazgo en ciberseguridad por parte de los ejecutivos puede resultar en decisiones estratégicas inadecuadas y una implementación deficiente de medidas de seguridad, lo que aumenta el riesgo de filtración de datos y daños a la reputación de la empresa.

Para abordar este desafío, se propone diseñar un programa de capacitación específico para los ejecutivos de la empresa. Este programa estará diseñado para cerrar la brecha de conocimiento en ciberseguridad y fortalecer la postura de seguridad de la empresa. Se basará en una revisión exhaustiva de la literatura en ciberseguridad y capacitación ejecutiva, con el objetivo de promover una cultura de seguridad en toda la organización y garantizar el cumplimiento de las regulaciones legales pertinentes.

Al cerrar la brecha de conocimiento en ciberseguridad y fortalecer la postura de seguridad de la empresa, esta investigación no solo beneficiará a la empresa, sino que también servirá como un modelo para otras organizaciones que enfrentan desafíos similares en un entorno empresarial cada vez más digitalizado y regulado.

2. Determinación del Problema

A pesar de las inversiones en tecnologías de seguridad y la implementación de medidas preventivas, la empresa enfrenta desafíos persistentes en la protección de datos. La existencia de regulaciones legales como la Ley Orgánica de Protección de Datos Personales y el Código Orgánico Integral Penal (COIP) en Ecuador, que establece sanciones para la violación de datos personales, subraya la importancia crítica de fortalecer la ciberseguridad en todas las organizaciones.

Se ha adoptado medidas proactivas para abordar estos desafíos. Sin embargo, a pesar de estos esfuerzos, persiste una brecha de conocimiento en ciberseguridad entre los ejecutivos y líderes empresariales.

Esta brecha de conocimiento representa un riesgo significativo para la empresa y sus clientes. La falta de comprensión profunda de las amenazas cibernéticas y las estrategias de seguridad necesarias por parte de los ejecutivos puede conducir a decisiones estratégicas inadecuadas y a una implementación deficiente de medidas de seguridad, lo que aumenta le probabilidad de violaciones de datos y daños a la reputación.

Por lo tanto, el problema identificado se centra en la necesidad de cerrar la brecha de conocimiento en ciberseguridad entre los ejecutivos y líderes empresariales de la empresa con el objetivo de fortalecer la postura de seguridad de la empresa y garantizar el cumplimiento de las regulaciones legales pertinentes. Esta investigación se propone diseñar un programa de capacitación específico para los ejecutivos, basado en una revisión exhaustiva de la literatura en ciberseguridad y capacitación ejecutiva, con el fin de promover una cultura de seguridad en toda la organización y mitigar los riesgos asociados con la protección de datos sensibles y personales de sus clientes.

Este estudio beneficiará a la compañía estudiada y se convertirá en un modelo para otras organizaciones que enfrentan desafíos similares en un entorno empresarial digitalizado y regulado.

3. Marco teórico referencial

En el contexto de la ciberseguridad empresarial y la capacitación ejecutiva, se explorarán diversas teorías, modelos y conceptos relevantes para comprender mejor el problema y diseñar una solución efectiva. A continuación, se presentan algunos elementos clave del marco teórico referencial:

3.1 Concepto de Ciberseguridad

Hace referencia a las acciones y tácticas implementadas para resguardar los sistemas informáticos, redes y datos frente a amenazas y ataques en línea. Se trata de un ámbito interdisciplinario que comprende aspectos técnicos, legales y políticos, y su relevancia continúa en aumento en un entorno cada vez más digitalizado. [4]

3.2 Ciberseguridad empresarial

Se examinarán los principios fundamentales de la ciberseguridad empresarial, incluyendo la prevención de amenazas, la protección de datos, la detección de intrusiones y la gestión de riesgos. Se explorarán modelos de seguridad de la información, como el modelo de seguridad de la información de ISO/IEC 27001, para comprender cómo las organizaciones pueden implementar un enfoque estructurado para proteger sus activos digitales.

3.3 Brecha de conocimiento en ciberseguridad

Se analizarán estudios previos y casos de investigación que han documentado la brecha de conocimiento en ciberseguridad entre los ejecutivos y líderes empresariales. Se explorarán las causas subyacentes de esta brecha, que pueden

incluir la falta de conciencia sobre las amenazas cibernéticas, la complejidad tecnológica y la falta de capacitación adecuada.

3.4 Capacitación ejecutiva en Ciberseguridad

Se revisarán las mejores prácticas y enfoques para la capacitación ejecutiva en ciberseguridad. Esto incluirá la identificación de necesidades de capacitación, el diseño de programas efectivos y la evaluación del impacto de la capacitación en el comportamiento y las prácticas de seguridad de los ejecutivos.

3.5 Teorías del aprendizaje organizacional

Se explorarán teorías del aprendizaje organizacional que pueden informar el diseño y la implementación de programas de capacitación en ciberseguridad. Esto puede incluir teorías como el Modelo de Aprendizaje Organizacional de Argyris y Schön, que enfatiza la importancia del aprendizaje continuo y la reflexión en la mejora de la seguridad organizacional.

3.6 Impacto de la brecha de conocimiento en la seguridad empresarial

Se analiza el impacto potencial de la brecha de conocimiento en ciberseguridad en la seguridad empresarial y la protección de datos de la empresa, así como en la credibilidad de los clientes y la imagen corporativa.

3.7 Regulaciones y marcos legales relacionados con la protección de datos

Analiza las regulaciones y marcos legales relevantes en materia de protección de datos en el contexto ecuatoriano, como la Ley Orgánica de Protección de Datos Personales y el Código Orgánico Integral Penal (COIP).

3.8 Norma ISO 27001

Según la página de la norma ISO: “Es un conjunto de requisitos y mejores prácticas destinados a garantizar la confidencialidad, integridad y disponibilidad de la información en una organización. Promueve un enfoque integral de la seguridad de la información, abarcando a las personas, las políticas y la tecnología”. [5]

4. ANTECEDENTES

Actualmente se han documentado numerosos casos donde se presentan casos relevantes sobre la fuga de datos y la importancia de evitar que esto suceda. A continuación, se presentan algunos antecedentes relevantes que respaldan la necesidad de esta investigación:

En el contexto de esta investigación, se destaca el caso de Equifax, una de las agencias de informes de crédito más prominentes a nivel mundial. En 2017, Equifax experimentó una de las brechas de seguridad más significativas hasta la fecha, que afectó a millones de personas en los Estados Unidos, Canadá y el Reino Unido.

La violación de seguridad de Equifax fue el resultado de una serie de vulnerabilidades en su software que no fueron abordadas a tiempo, lo que permitió a los ciberdelincuentes acceder a información personal sensible, incluyendo nombres, números de seguro social, fechas de nacimiento y direcciones. Este incidente no solo causó un daño significativo a la reputación de Equifax, sino que también generó preocupaciones sobre la responsabilidad de las empresas en la protección de los datos de sus clientes y la necesidad de contar con medidas de seguridad sólidas y planes de respuesta ante incidentes efectivos. [6]

Adicional resalta el alarmante incidente de filtración masiva de datos en Ecuador, generando preocupación a nivel nacional e internacional.

El incidente, revelado en informes de la BBC y vpnMentor, expuso información altamente sensible de aproximadamente 20 millones de ciudadanos ecuatorianos, incluyendo nombres, direcciones, números de teléfono, datos financieros y de vehículos, entre otros detalles personales. Esta filtración, detectada en un servidor ubicado en Miami, EE. UU., y gestionado presuntamente por la empresa ecuatoriana Novaestrat, ha generado preocupaciones significativas sobre la seguridad y privacidad de los datos en el país.

Lo alarmante de esta brecha de seguridad radica en su alcance y en la diversidad de fuentes de las cuales proviene la información filtrada, que abarca bases de datos gubernamentales, registros financieros y datos de empresas ecuatorianas. Aunque la filtración fue detectada y cerrada en septiembre de 2019 por expertos de vpnMentor, los riesgos persisten para los individuos cuyos datos fueron expuestos, quienes podrían enfrentarse a amenazas continuas de estafas, fraudes financieros y robo de identidad.

Este incidente subraya la necesidad apremiante de adoptar medidas más estrictas de seguridad de datos tanto a nivel gubernamental como en el sector privado, así como de promover una mayor conciencia sobre la importancia de proteger la privacidad de la información personal. En este contexto, surge la relevancia de investigaciones que aborden los desafíos y las soluciones en materia de seguridad de datos en Ecuador, con el objetivo de fortalecer las políticas y prácticas que garanticen la integridad y confidencialidad de la información personal en el país. [7]

En marzo de 2024, la empresa enfrentó un incidente de fuga de datos cuando un excolaborador, que trabajó como gestor de cobranza durante la pandemia, subió una base con información sensible a Scribd, una plataforma de documentos digitales. Aunque las circunstancias detrás de esta acción no están claras, se logró resolver el problema al contactar directamente al excolaborador, quien eliminó la información compartida.

Se presentaron tres incidentes significativos de robo de información sensible: uno a nivel global, como el caso de Equifax, otro a nivel nacional y un tercero que afectó directamente a la empresa. Estos eventos subrayan la vulnerabilidad de cualquier empresa frente a ataques que pueden resultar en la filtración de datos sensibles, con consecuencias legales y de reputación para la empresa afectada. Es crucial que los altos directivos estén conscientes de estos riesgos y asignen los recursos necesarios para implementar medidas de seguridad adecuadas y prevenir futuros incidentes.

5. JUSTIFICACIÓN

La ciberseguridad se ha convertido en una preocupación fundamental para las empresas en la era digital actual. Los ataques cibernéticos, cada vez más sofisticados, pueden comprometer la seguridad de la información, la continuidad operativa y la reputación de una empresa. Por esta razón, es crucial que los ejecutivos comprendan la importancia de la ciberseguridad y estén preparados para liderar la implementación de medidas eficientes de protección en sus organizaciones. Los empleados están, en consecuencia, expuestos a diversas amenazas de ciberseguridad que podrían tener efectos adversos impactos en sus organizaciones. [8]

Este proyecto propone un programa de capacitación específico dirigido a los ejecutivos de la empresa con el objetivo de transformar su enfoque hacia la ciberseguridad y empoderarlos para liderar iniciativas efectivas en sus respectivas empresas. La capacitación resalta la importancia estratégica de la ciberseguridad, proporcionando a los ejecutivos una comprensión profunda de cómo los ciberataques pueden afectar a la empresa a largo plazo. Además, capacita a los líderes empresariales para establecer una cultura organizacional que fomente la conciencia y el cumplimiento de las políticas de seguridad.

El programa proporciona a los ejecutivos la capacidad de tomar decisiones informadas en cuanto a la inversión en seguridad, minimizando el impacto de los incidentes de seguridad y garantizando un cumplimiento normativo adecuado. En resumen, esta propuesta de enseñanza de ciberseguridad para ejecutivos busca mejorar la seguridad digital en las empresas, empoderando a los líderes y ejecutivos para que comprendan los riesgos cibernéticos y tomen decisiones informadas en materia de ciberseguridad, convirtiéndola en una prioridad estratégica en todas las áreas de la empresa.

6. Objetivos (General y específicos)

Objetivo general

Desarrollar un programa de capacitación en ciberseguridad para los ejecutivos de la empresa con el fin de fortalecer su comprensión y liderazgo en esta área.

Objetivos especificos

- Identificar las necesidades de capacitación en ciberseguridad de los ejecutivos.
- Crear un programa de capacitación que aborde las necesidades.
- Implementar el programa de capacitación de manera efectiva para garantizar el compromiso y la comprensión de los ejecutivos.

7. Marco teórico referencial

Para respaldar este estudio, resulta crucial establecer las siguientes definiciones:

7.1 Ciberseguridad

Se considera a la ciberseguridad como un "conjunto de variables claves, acertadamente definidas por la ITU – International Telecomunication Unión – en las cuales son necesarias el desarrollo de prácticas primordiales para darle sentido y real dimensión a la seguridad de una nación". [9]

7.2 Riesgos cibernéticos

Los riesgos cibernéticos son amenazas y vulnerabilidades que pueden resultar en la exposición de datos y sistemas a ataques cibernéticos. Esto incluye amenazas como malware, phishing, ataques de denegación de servicio (DDos) y brechas de seguridad. [10]

7.3 Cultura de seguridad

La cultura de seguridad abarca los valores, actitudes y acciones que una organización adopta respecto a la seguridad cibernética. Una cultura de seguridad robusta fomenta la conciencia y la responsabilidad en todos los niveles de la empresa.

7.4 Brecha de conocimiento

La brecha de conocimiento en ciberseguridad se refiere a la falta de comprensión y conocimiento de las amenazas cibernéticas, estrategias de seguridad y prácticas efectivas entre los líderes empresariales, lo que resulta en decisiones estratégicas inadecuadas y una falta de liderazgo en ciberseguridad.

8. METODOLOGÍA

La metodología propuesta para llevar a cabo esta investigación se basará en un enfoque mixto, combinando métodos cualitativos y cuantitativos, enfocándonos en el modelo ADDIE, para obtener una comprensión integral de las necesidades de capacitación en ciberseguridad de los ejecutivos y evaluar la efectividad del programa de capacitación propuesto. Este modelo ayuda a identificar necesidades de capacitación, diseñar planes de aprendizaje, desarrollar materiales educativos, implementar programas de capacitación y evaluar su efectividad [11]. A continuación, se describen los pasos metodológicos:

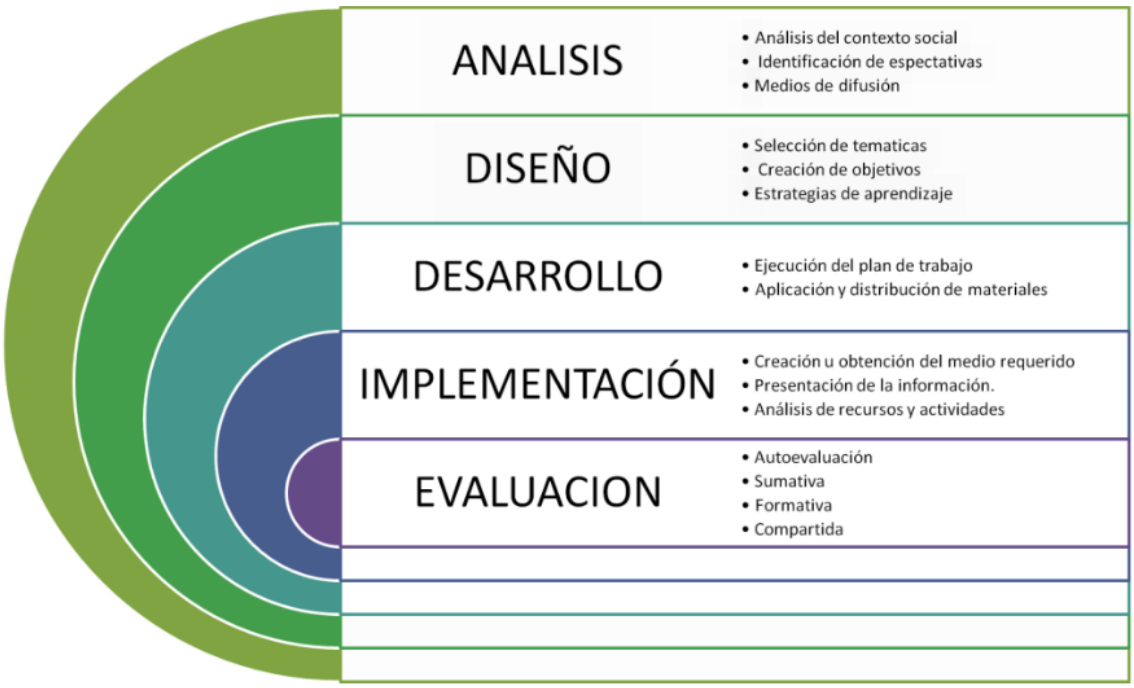

Ilustración 1 - MODELO ADDIE

8.1 ANÁLISIS DE NECESIDADES DE CAPACITACIÓN

Se realizará una investigación cualitativa para identificar las necesidades de capacitación en ciberseguridad de los ejecutivos de la empresa. Se llevarán a cabo

entrevistas semiestructuradas con ejecutivos clave y se aplicarán cuestionarios para recopilar información sobre su comprensión actual de la ciberseguridad, áreas de interés y necesidades de capacitación específicas.

Actualmente el organigrama estructural de la empresa se expresa de esta manera:

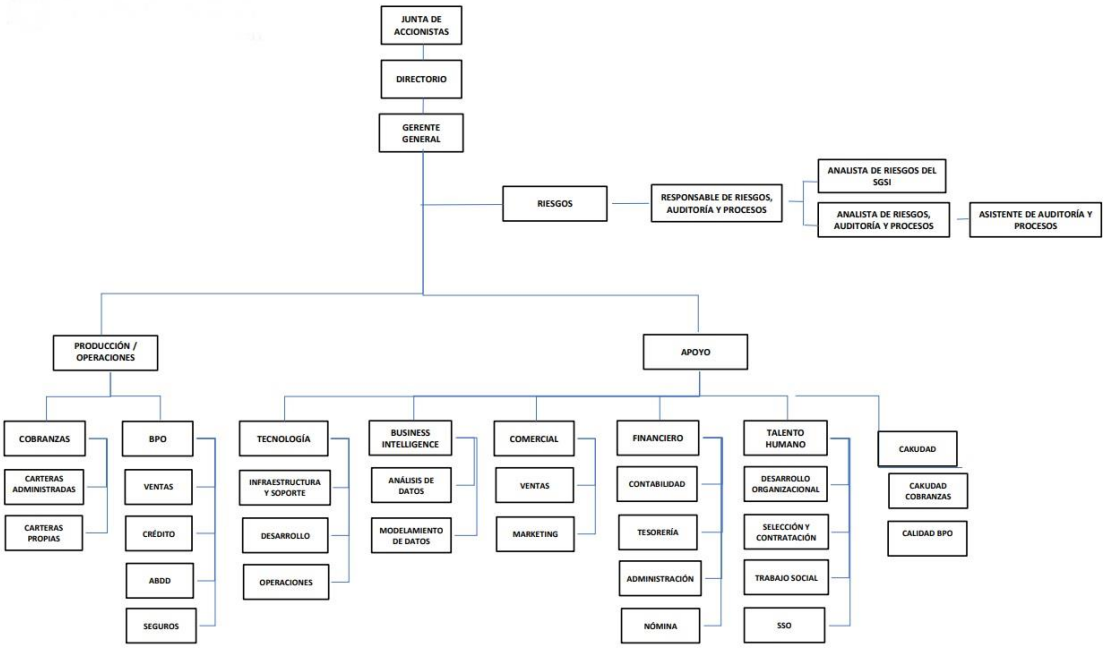

Ilustración 2 - Organigrama

Los ejecutivos en los cuales se tomarán las muestras serían el Gerente General, Jefe de Riesgos, Cobranzas, Tecnología, Business Intelligence, Comercial, Financiero, Talento Humano, Calidad y Supervisores que manejan personal.

8.2 Diseño y desarrollo del programa de capacitación

Para diseñar y desarrollar el programa de capacitación, se analizarán los resultados de entrevistas y cuestionarios para identificar las áreas de mejora de los ejecutivos. Se impartirán charlas centradas en temas generales de ciberseguridad y leyes

ecuatorianas relevantes, con un enfoque particular en artículos que puedan representar riesgos para la empresa.

Además, el programa incluirá la creación de materiales de apoyo, como carteles informativos colocados estratégicamente en áreas clave de la empresa, para proporcionar información importante sobre seguridad de la información.

8.3 Implementación del programa de capacitación

La implementación del programa de capacitación en ciberseguridad requiere una planificación detallada, comunicación interna efectiva y el desarrollo de materiales de apoyo. Durante las charlas, se deben abordar temas relevantes de manera práctica y realista, y recopilar comentarios para evaluar y ajustar el programa según sea necesario. Es crucial mantenerse actualizado con las regulaciones y actualizar el contenido de las sesiones para garantizar su relevancia a lo largo del tiempo.

8.4 Evaluación de la efectividad del programa

La evaluación de la efectividad del programa de capacitación en ciberseguridad se llevará a cabo mediante pruebas de conocimientos antes y después de las sesiones, encuestas de satisfacción para recopilar opiniones sobre la calidad del programa, y análisis de la participación y comportamiento de los ejecutivos. También es útil realizar un seguimiento a largo plazo para evaluar el impacto continuo del programa en la seguridad de la empresa y en la conciencia de ciberseguridad de los participantes. Utilizando una combinación de estas técnicas de evaluación, se

obtendrá una visión completa de la efectividad del programa y realizar ajustes necesarios para mejorar su impacto en la protección de la información empresarial.

8.5 Análisis de datos y elaboración de conclusiones

El análisis de datos y la elaboración de conclusiones del programa de capacitación en ciberseguridad implicarían inicialmente la recopilación y organización sistemática de los datos obtenidos durante la evaluación, incluyendo resultados de pruebas, respuestas de encuestas, registros de participación y observaciones. Posteriormente, se llevaría a cabo un análisis detallado de estos datos, empleando tanto métodos estadísticos como análisis cualitativos para identificar tendencias, patrones significativos y diferencias entre grupos de participantes. A partir de este análisis, se interpretarían los resultados en el contexto de los objetivos del programa y se extraerían conclusiones sobre su efectividad, resaltando aspectos positivos y áreas de mejora.

Con base en las conclusiones obtenidas, se elaborarían recomendaciones específicas para fortalecer el programa en futuras iteraciones. Estas recomendaciones podrían abarcar ajustes en el contenido y formato de las sesiones, así como sugerencias para mejorar la participación y la eficacia del programa. Además, se destacarían áreas de éxito que puedan ser replicadas en otros contextos, así como aspectos identificados como prioritarios para abordar en futuras mejoras del programa.

9. Cronograma de actividades

1. **Fase de Investigación (Semana 1)**

- **Actividades:**

    - Revisión de literatura sobre ciberseguridad en el entorno empresarial.
    - Análisis de la situación actual de la empresa. en cuanto a ciberseguridad.
    - Identificación de regulaciones legales pertinentes en Ecuador.
    - Entrevistas con ejecutivos y líderes empresariales de la empresa para comprender sus necesidades de capacitación en ciberseguridad.

2. **Fase de Diseño del Programa de Capacitación (Semana 2)**

    - **Actividades:**
        - Consolidación de los hallazgos de la investigación.
        - Desarrollo del contenido del programa de capacitación en base a las necesidades identificadas.
        - Diseño de materiales didácticos y recursos de aprendizaje.
        - Definición de metodologías de enseñanza y evaluación.

3. **Fase de Implementación del Programa (Semana 3)**

    - **Actividades:**
        - Preparación de la infraestructura necesaria para la capacitación (plataforma en línea, salones de capacitación, etc.).
        - Selección de ejecutivos participantes en el programa.
        - Impartición del programa de capacitación en sesiones presenciales o virtuales.
        - Seguimiento y apoyo continuo a los participantes durante el proceso de capacitación.

4. **Fase de Evaluación y Ajustes (Semana 4)**
    - **Actividades:**

- Recopilación de retroalimentación de los ejecutivos participantes.
- Evaluación del impacto del programa en el conocimiento y liderazgo en ciberseguridad de los ejecutivos.
- Análisis de los resultados obtenidos y comparación con los objetivos establecidos.
- Realización de ajustes y mejoras al programa según sea necesario.

5. **Fase de Documentación y Presentación de Resultados (Semana 5)**

- **Actividades:**
  - Elaboración del informe final de la tesis, incluyendo introducción, determinación del problema, justificación, objetivos, resultados y conclusiones.
  - Preparación de la presentación oral de la tesis.
  - Entrega del informe final y presentación ante el comité evaluador.

6. **Fase de Divulgación y Implementación (Semana 6)**

- **Actividades:**
  - Publicación de los resultados de la tesis en revistas académicas o conferencias relacionadas.
  - Comunicación de los hallazgos y recomendaciones a la empresa.
  - Apoyo en la implementación de las recomendaciones derivadas de la investigación.

10. Resultados y discusión

10.1 Evaluación del nivel de comprensión

Para evaluar el nivel de comprensión de los ejecutivos en ciberseguridad, se realizaron entrevistas y encuestas. Los resultados indicaron que, en su mayoría, los ejecutivos tenían una comprensión limitada de las amenazas cibernéticas y las estrategias de seguridad que actualmente está implementado en la empresa, adicional muestran desconocimiento en las preguntas realizadas en el tema de leyes que actualmente rigen en el Ecuador, destacando desconocimiento que cualquier cargo puede estar expuesto a estos problemas penales. Este hallazgo destaca la necesidad crítica de implementar un programa de capacitación en ciberseguridad.

10.2 Modelo de las preguntas realizadas en la entrevista

1. **Conocimiento de Leyes**
    - ¿Está familiarizado con la Ley Orgánica de Protección de Datos Personales y el Código Orgánico Integral Penal (COIP) en Ecuador?
2. **Comprensión de Obligaciones**
    - ¿Qué medidas toma la empresa para asegurar el cumplimiento de las leyes de protección de datos en Ecuador?
3. **Responsabilidades Legales**
    - ¿Cuál es su comprensión sobre las responsabilidades legales y sanciones asociadas a la violación de las leyes de protección de datos en Ecuador?

4. **Familiaridad con sistemas de prevención de datos**
    - ¿Está al tanto de los sistemas de prevención de pérdida de datos utilizados en la empresa?
    - ¿Conoce usted que es un Sistema de Gestión en Seguridad de la Información (SGSI)?

- ¿Conoce usted la existencia del Sistema de Gestión en Seguridad de la Información (SGSI)?

5. **Importancia de Implementación de Sistemas de protección de datos**
    - Desde su perspectiva, ¿cuál es la importancia de implementar sistemas de protección de datos en una empresa?
6. **Evaluación de Efectividad**
    - ¿Cómo evalúa usted la efectividad de los sistemas que actualmente se encuentran implementados en la empresa?
7. **Iniciativas de Capacitación**

    - ¿Existe algún programa de capacitación o formación para los empleados sobre la importancia y uso de los sistemas de protección de datos?

10.3 Modelo de las preguntas realizadas en la encuesta

1. **¿Está familiarizado con la Ley Orgánica de Protección de Datos Personales y el Código Orgánico Integral Penal (COIP) en Ecuador?**
    - Si
    - No
2. **¿Qué medidas toma la empresa para asegurar el cumplimiento de las leyes de protección de datos en Ecuador? Puede escoger más de una respuesta.**
    - Implementación de políticas de privacidad.
    - Capacitación regular a empleados.
    - Auditorías de cumplimiento.
    - No toma ninguna medida.
3. **¿Conoce sus responsabilidades legales y sanciones asociadas a la violación de las leyes de protección de datos en Ecuador?**
    - Si
    - No

4. **¿Qué sanciones constan en la Ley de Protección de Datos en el Ecuador? Puede escoger más de una respuesta.**
    - Pérdida de licencia comercial.
    - Multas económicas.
    - Sanciones penales.
5. **¿Está al tanto de los sistemas de Prevención de Pérdida de Datos que serán implementados en la empresa?**
    - Si
    - No
6. **Desde su perspectiva, ¿cuál es la importancia de implementar sistemas de protección de datos en una empresa? Puede escoger más de una respuesta**
    - Proteger datos sensibles.
    - Cumplir con regulaciones legales.
    - Prevenir fugas de información.
7. **¿Considera que es efectiva la de protección de datos implementados actualmente en la empresa?**
    - Si
    - No
8. **¿Conoce usted si existe algún programa de capacitación o formación para los empleados sobre la importancia y uso de los sistemas de protección de datos en la empresa?**
    - Si
    - No
9. **Si su respuesta fue afirmativa, Escoja de las siguientes respuestas las capacitaciones que usted ha recibido:**
    - Protección de Datos Personales
    - Sistema de Gestión de Seguridad de la Información
    - Política de contraseña
    - Otra

10.4 Diseño del plan de capacitación

El diseño del plan de capacitación se fundamentó en los resultados obtenidos de la evaluación del nivel de comprensión. Se desarrollaron módulos temáticos desde conceptos básicos hasta estrategias avanzadas de ciberseguridad, con la inclusión de métodos visuales, como carteles estratégicamente ubicados, junto con enfoques tradicionales como clases magistrales, ejercicios prácticos y estudios de casos.

El modulo temático se estableció de esta manera:

	Tema	Objetivo	Metodología
Modulo 1	Introducción a la Ciberseguridad	Establecer fundamentos básicos sobre amenazas cibernéticas y vulnerabilidades comunes.	Clases magistrales para presentar conceptos clave y ejercicios prácticos para identificar y manejar riesgos básicos.
Modulo 2	Leyes y Normativas Relevantes	Familiarizar a los ejecutivos con la Ley Orgánica de Protección de Datos Personales y el Código Orgánico Integral Penal (COIP) de Ecuador.	Estudios de casos basados en situaciones legales actuales y discusiones sobre responsabilidades legales y sanciones.
Modulo 3	Gestión de Riesgos y Cumplimiento	Capacitar a los ejecutivos en la identificación proactiva de riesgos y en la implementación de políticas de cumplimiento.	Simulaciones de escenarios de amenazas, donde los ejecutivos deben diseñar estrategias de mitigación y cumplimiento.
Modulo 4	Tecnologías y Herramientas de Seguridad	Explorar herramientas avanzadas de seguridad cibernética y su aplicación práctica en la protección de datos empresariales.	Talleres prácticos para la configuración y gestión de herramientas de prevención de pérdida de datos y sistemas de gestión de seguridad de la información (SGSI).

Tabla 1 - Modulo Temático

Cada módulo y método de enseñanza ha sido seleccionado y diseñado específicamente para abordar las áreas de mejora identificadas durante la evaluación inicial del nivel de comprensión en ciberseguridad. Los temas y enfoques fueron ajustados para asegurar que los ejecutivos adquieran las habilidades necesarias para liderar iniciativas de seguridad cibernética dentro de la empresa.

10.5 DISEÑO DE LA SOLUCIÓN

Después de analizar las encuestas y entrevistas, identificamos una falta de comprensión entre los ejecutivos en áreas críticas como la función de un Sistema de Gestión en Seguridad de la Información, la protección de datos personales y la comprensión de las obligaciones y leyes pertinentes que podrían impactar a la empresa. Como respuesta a este desafío, diseñamos un enfoque específico para la capacitación, abordando estos puntos clave de manera detallada y práctica.

Para abordar esta brecha de conocimiento, creamos materiales y recursos que incluyeron presentaciones informativas durante las sesiones de capacitación, así como métodos visuales como carteles estratégicamente ubicados. Estos materiales se diseñaron cuidadosamente para ser accesibles y comprensibles, evitando el uso de un lenguaje técnico excesivo que pudiera dificultar la participación efectiva de los ejecutivos.

10.5.1 FUNCIONAMIENTO DE SEGURIDAD DE LA INFORMACIÓN

Con el fin de reducir el desconocimiento generalizado sobre la seguridad de la información, se crearon presentaciones y materiales informativos que se centran en proporcionar un entendimiento claro de las soluciones disponibles. Estos recursos destacan los pilares esenciales de un Sistema de Gestión en Seguridad de la Información, las políticas de cumplimiento y el rol crucial de la norma ISO 27001. Este enfoque ha resultado en una notable disminución de la brecha de conocimiento en este tema.

Ilustración 3 – Capacitación SGSI

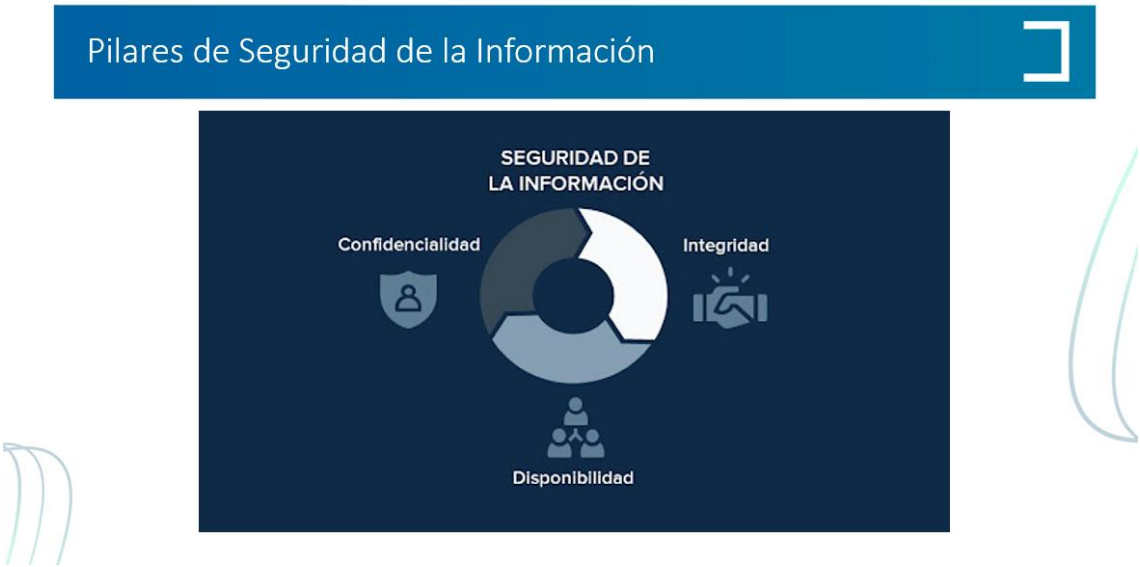

Ilustración 4 – Capacitación Pilares SGSI

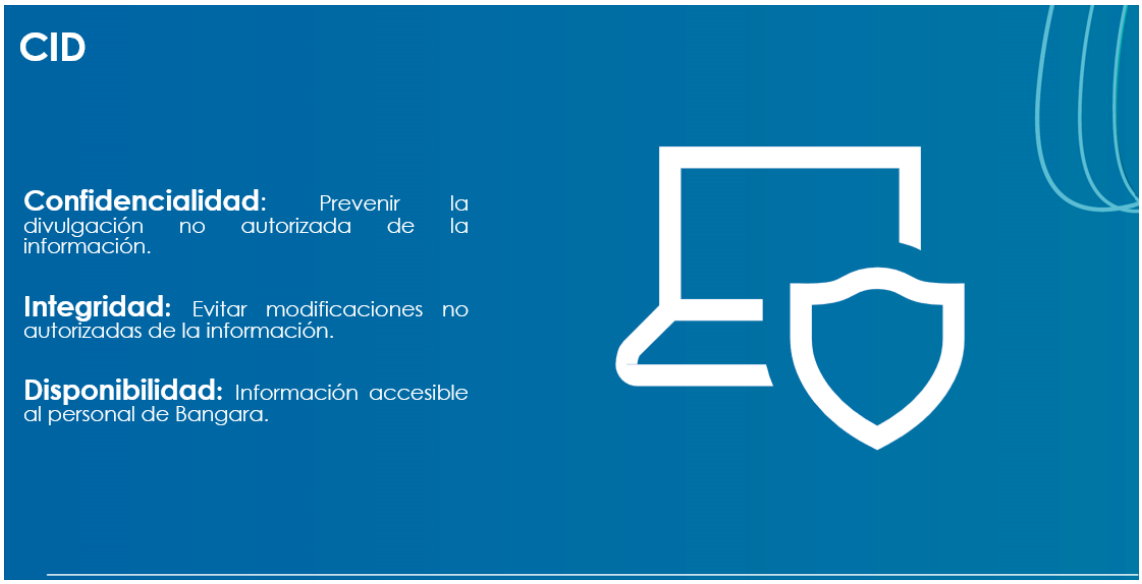

Ilustración 5 – Capacitación Pilares SGSI 2

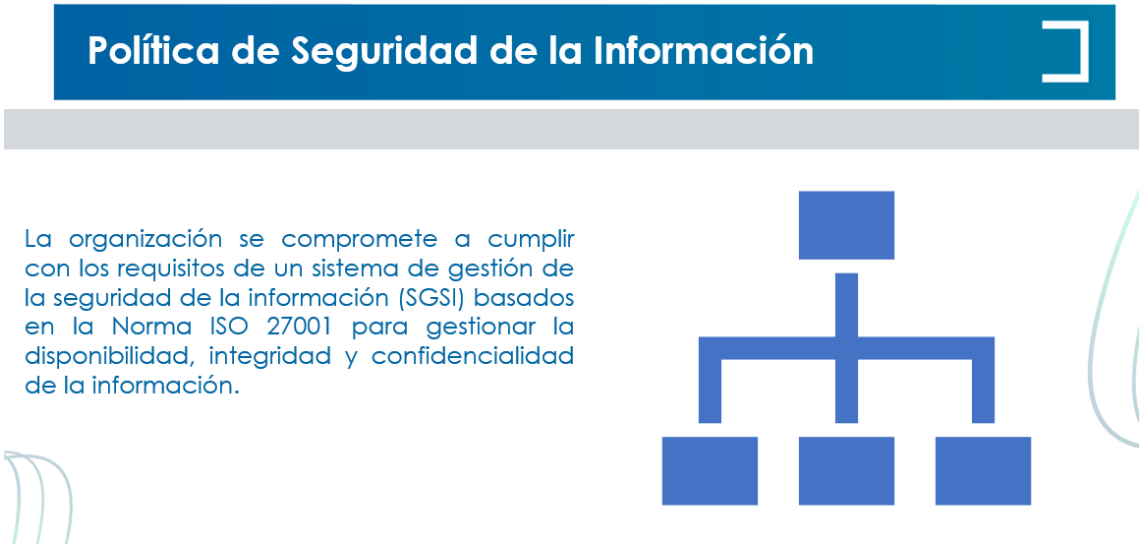

Ilustración 6 – Capacitación Políticas

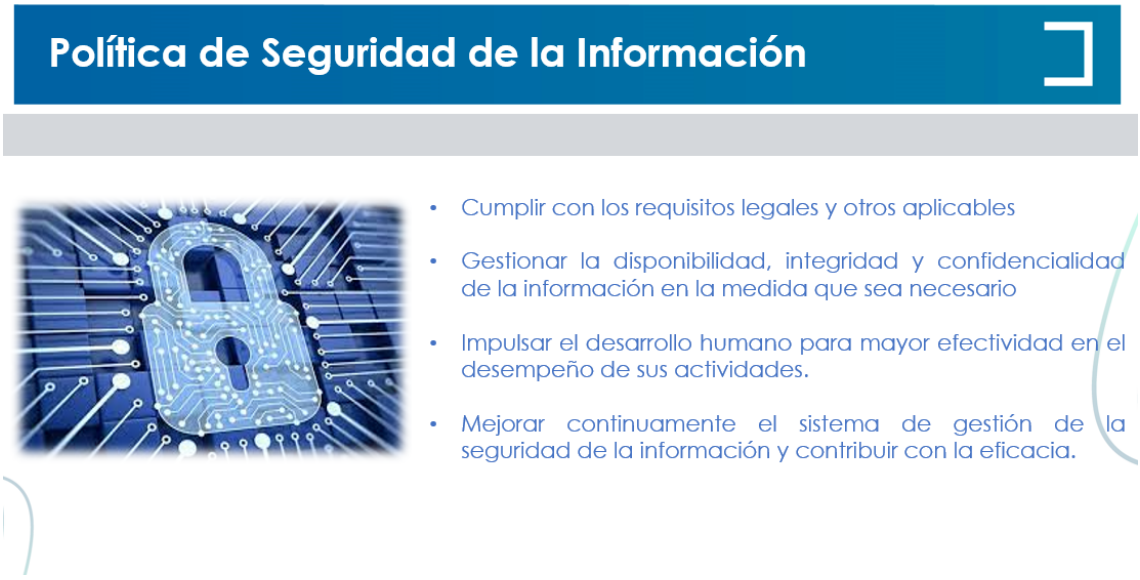

Ilustración 7 – Capacitación Políticas 2

Se muestran algunos casos de la información plasmada mediante carteleras y tendones:

Ilustración 8– Material de concientización

Se evidencio un impacto significativo en el personal de la empresa, con testimonios directos que destacaron cómo los materiales y recursos utilizados mejoraron la comprensión de la función de la seguridad de la información y aumentaron el conocimiento sobre la certificación ISO 27001 que posee la empresa. Este feedback se obtuvo inmediatamente al recopilar opiniones directas sobre la efectividad de estos recursos, los cuales fueron ubicados estratégicamente para que los ejecutivos tuvieran acceso visual directo a esta información.

10.5.2 Protección de datos personales

Para abordar la falta de comprensión en torno a la protección de datos personales, creamos presentaciones específicamente diseñadas para proporcionar claridad sobre este tema. Estos recursos resaltan la importancia de proteger los datos personales y destacan las medidas de seguridad necesarias para garantizar el cumplimiento normativo. Como resultado, se observó una notable mejora en la comprensión y conciencia de los ejecutivos sobre la protección de datos personales.

Ilustración 9 – Datos personales

Ilustración 10 – Capacitación Datos Personales 2

Ilustración 11 – Capacitación Ley

10.5.3 Protección de datos personales

Para enfrentar la falta de comprensión sobre las obligaciones legales y las leyes que podrían impactar a la empresa, se crearon presentaciones que destacan los aspectos clave de la legislación. Estos recursos proporcionan información detallada sobre las leyes, como el Código Orgánico Integral Penal y la Ley Orgánica de Protección de Datos Personales, con especial énfasis en el artículo 47 de esta. Dado

que la empresa actúa como responsable y encargada del tratamiento de datos personales, se enfoca en implementar técnicas, administrativas y jurídicas adecuadas, realizar evaluaciones periódicas de seguridad, y notificar de manera apropiada a las autoridades competentes y a los titulares de los datos en caso de incidentes de seguridad, lo cual el artículo hace referencia.

Además, se enfatizan las responsabilidades legales asociadas con el incumplimiento de estas leyes y las posibles sanciones. Esta iniciativa ha contribuido significativamente a mejorar la comprensión de los ejecutivos sobre sus obligaciones legales y los riesgos asociados, fortaleciendo así la postura de cumplimiento legal de la empresa.

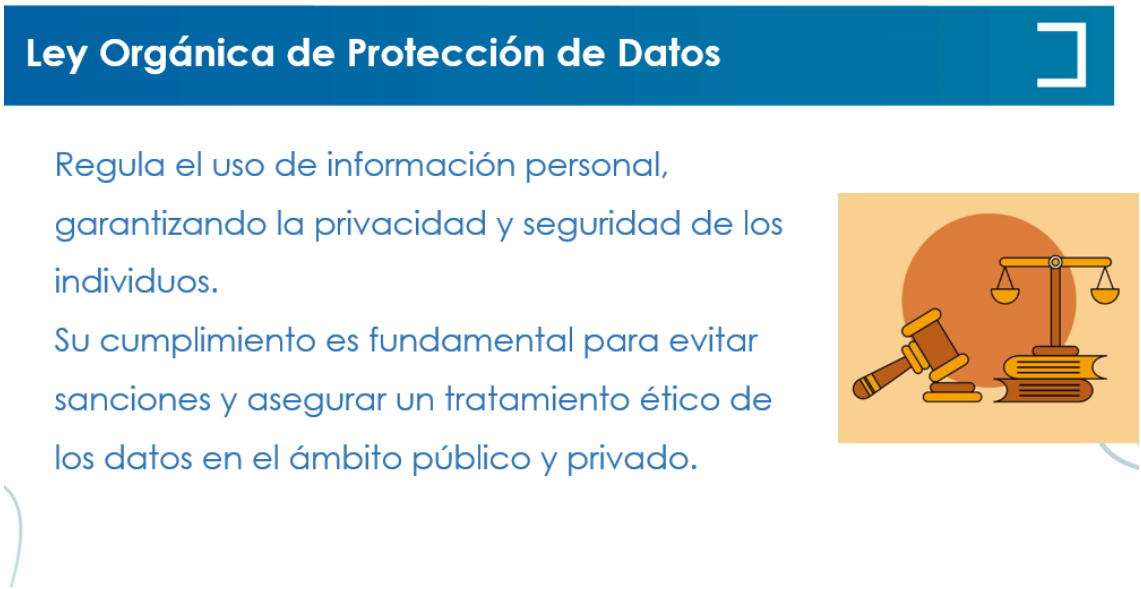

Ilustración 11 – Capacitación Ley

LOPDP

Art. 34.-Acceso a datos personales por parte del encargado.-No se considerará transferencia o comunicación en el caso de que el encargado acceda a datos personales para la prestación de un servicio al responsable del tratamiento de datos personales. El tercero que ha accedido legítimamente a datos personales en estas consideraciones, será considerado encargado del tratamiento.

El tratamiento de datos personales realizado por el encargado deberá estar regulado por un contrato, en el que se establezca de manera clara y precisa que el encargado del tratamiento de datos personales tratará únicamente los mismos conforme las instrucciones del responsable y que no los utilizará para finalidades diferentes a las señaladas en el contrato, ni que los transferirá o comunicará ni siquiera para su conservación a otras personas.

Una vez que se haya cumplido la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento de datos personales bajo la supervisión de la Autoridad de Protección de Datos Personales.

El encargado será responsable de las infracciones derivadas del incumplimiento de las condiciones de tratamiento de datos personales establecidas en la presente ley.

Ilustración 11 – Capacitación Ley

Código Orgánico Integral Penal

Es un cuerpo legal que recopila y regula las leyes penales de un país.

Establece normas y procedimientos para la aplicación de la justicia penal, abordando delitos, penas y garantías procesales en un marco legal integral

Ilustración 12 – Capacitación COIP

Código Orgánico Integral Penal

Art. 178.- Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.

Ilustración 12 – Capacitación COIP

10.6 RESULTADOS CLAVES

Se volvieron a realizar las encuestas y entrevistas a los ejecutivos después de las capacitaciones, donde se identificaron indicadores claros de mejora en su comprensión sobre la importancia de la protección de datos en la empresa. Los resultados de estas evaluaciones indicaron un impacto positivo de las capacitaciones en la percepción y conocimiento de los ejecutivos, destacando una mayor conciencia sobre los desafíos relacionados seguridad de la información.

- Los ejecutivos mostraron mayor interés y conciencia sobre la importancia estratégica de la ciberseguridad en la empresa
- Hubo una mejora en la capacidad de los ejecutivos para tomar decisiones informadas en inversiones de seguridad y liderar iniciativas de protección

	Nivel de comprensión (Antes)	**Nivel de comprensión (Después)**
Conocimiento de leyes	2	8
Comprensión de obligaciones	4	9
Responsabilidades legales	3	8

Familiaridad con sistemas de prevención de datos	3	10
Importancia de implementación de sistemas de protección de datos	5	10
Evaluación de efectividad	6	9
Iniciativas de capacitación	7	10

Ilustración 13 – Tabla comparativa

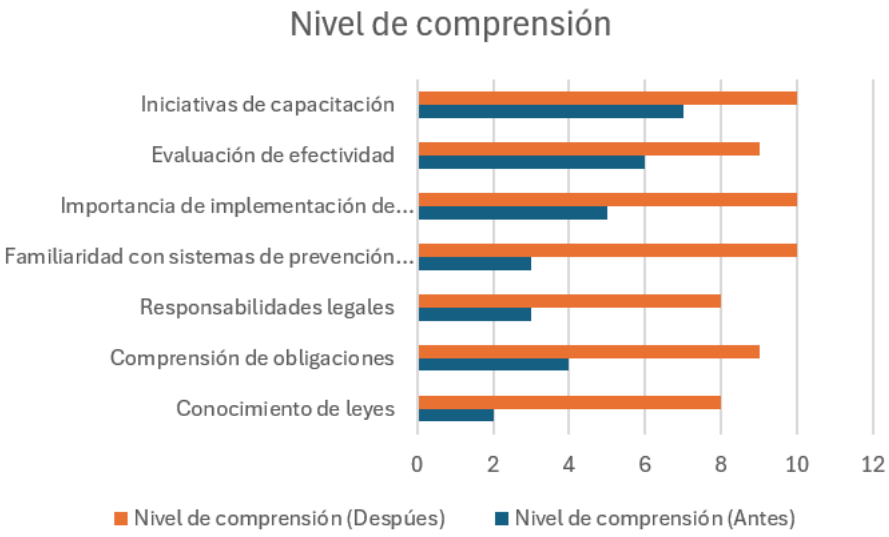

Ilustración 14 – Gráfico comparativo

10.7 Discusión

Los resultados refuerzan la importancia y eficacia del programa de capacitación diseñado. La transformación en la comprensión y actitud de los ejecutivos destaca la necesidad de abordar la brecha de conocimiento en ciberseguridad en el nivel de liderazgo. Este cambio positivo contribuirá a fortalecer la postura de seguridad cibernética en la organización.

La participación de los ejecutivos en la capacitación demuestra un reconocimiento creciente de la ciberseguridad como una prioridad estratégica. La mejora en la toma de decisiones y la capacidad para liderar iniciativas de seguridad indican un impacto positivo en la cultura de seguridad de las empresas.

10.8 Limitaciones y posibles fuentes de error

La investigación se centró en un grupo específico de ejecutivos, lo que podría limitar la generalización de los resultados. La evaluación del nivel de comprensión se basó en la percepción de los ejecutivos, lo que podría influir en la precisión de los resultados

A pesar de estas limitaciones, los resultados sugieren que el programa de capacitación es efectivo y puede adaptarse para abordar las brechas de conocimiento en ciberseguridad en diferentes contextos empresariales. Estas conclusiones respaldan la relevancia y necesitada continua de programas de este tipo para fortalecer la seguridad digital en el ámbito empresarial.

11. CONCLUSIONES

La investigación realizada se centra en abordar la brecha de conocimiento en ciberseguridad entre los ejecutivos y líderes empresariales, con un enfoque específico en el diseño e implementación de un programa de capacitación. Los resultados obtenidos rebelan varios aspectos importantes que destacan la necesidad de transformación en este ámbito.

En primer lugar, se destaca la importancia de una transformación efectiva del enfoque de los ejecutivos hacia la ciberseguridad. Esto implica integrar la legislación pertinente, como la Ley Orgánica de Protección de Datos Personales y el Código Orgánico Integral Penal, en las prácticas empresariales y judiciales. Más que simplemente cumplir con regulaciones legales, se busca promover una cultura organizacional y judicial que respete la privacidad y protección de datos, lo que requiere una capacitación y concientización adecuadas sobre estos aspectos.

Además, se subraya la importancia estratégica que los ejecutivos ahora asignan a la ciberseguridad, evidenciada por su participación en el programa de capacitación. Esta conciencia mejorada influye positivamente en la toma de decisiones, la asignación de recursos y la promoción de una cultura de seguridad en las organizaciones.

Los resultados también resaltan la relevancia crítica de abordar esta brecha de conocimiento en ciberseguridad a nivel de liderazgo. La seguridad digital ya no se puede considerar únicamente como un problema técnico, sino como una prioridad estratégica que requiere la participación y comprensión de los ejecutivos.

Finalmente, se proponen recomendaciones para continuar avanzando en este campo, como explorar la sostenibilidad a largo plazo de la transformación en la comprensión y actitud de los ejecutivos, investigar la adaptabilidad del programa de capacitación a diferentes sectores y contextos empresariales, y evaluar la

transferencia de conocimientos a través de los ejecutivos a otros niveles organizativos.

La investigación resalta la efectividad de un programa de capacitación específico para ejecutivos en cerrar la brecha de conocimiento en ciberseguridad. Este enfoque tiene el potencial de fortalecer significativamente la postura de seguridad cibernética en las empresas, contribuyendo así a la protección de información y la continuidad operativa en un entorno empresarial cada vez más digitalizado.

Referencias

[1] G. d. Ecuador, Ley de Organica de Protección de Datos Personales, Art. 37, "Seguridad de datos personales", 2021.

[2] G. d. Ecuador, Código Orgánico Integral Penal, Art. 178, "Delitos contra el derecho a la intimidad personal y familiar", 2021.

[3] E. F. Allauca Carrillo, *Propuesta de mejores prácticas de ciberseguridad para la comunicación en redes de clientes corporativos,* Ecuador, Ambato, 2022.

[4] N. M. y. M. Gazapo, «redalyc,» 10 2016. [En línea]. Available: https://www.redalyc.org/pdf/767/76747805002.pdf. [Último acceso: 21 04 2024].

[5] ISO, «ISO,» 2024. [En línea]. Available: https://www.iso.org/es/contents/data/standard/08/28/82875.html?tid=331662889277. [Último acceso: 21 04 2024].

[6] G. Norman, «PreyProject,» 11 07 2020. [En línea]. Available: https://preyproject.com/es/blog/la-brecha-a-equifax-que-aprendimos-sobre-nuestros-datos. [Último acceso: 17 04 2024].

[7] B. N. Mundo, «bbc.com,» BBC, 16 09 2019. [En línea]. Available: https://www.bbc.com/mundo/noticias-america-latina-49721456. [Último acceso: 17 04 2024].

[8] N. H. y. S. H. A. Aighazo, *Procedural Information Security Countermeasure Awareness and Cybersecurity Protection Motivation in Enhancing Employee´s Cybersecutity Protective Behaviour,* Malasia: 10th International Symposium on Digital Forensics and Security, 2022.

[9] T. G. y. T. Joseph, *Cybersecurity for executives a practical guide,* Nueva Jersey: John Wiley & Sons, Inc., 2014.

[10] C. Larry, *Cibersecurity for business,* Nueva York, Estados Unidos: Jellyfish, 2022.

[11] C. Aguilera, «ispring,» 28 04 2023. [En línea]. Available: https://www.ispring.es/blog/modelo-addie. [Último acceso: 21 04 2024].