Pontificia Universidad Católica del Ecuador

Facultad De Ingeniería

Escuela de Sistemas

TEMA:

ANALISIS DE VULNERABILIDADES Y MITIGACIÓN DE RIESGOS RELACIONADOS A LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA URBAN LAB EFFECT S.A.S.

AUTOR:

JOSUÉ IVÁN MOLINA GONZAGA

TRABAJO PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS Y COMPUTACIÓN

QUITO, 11 de junio del 2023.

DEDICATORIA

A mis padres, hermano y abuelos,

Este trabajo de culminación de mis estudios es el resultado de un largo camino universitario en el que su amor, apoyo incondicional, cariño y confianza han sido fundamentales. Gracias por siempre estar a mi lado en cada etapa, por inspirarme siempre y por nunca dejar de creer en mí. Este trabajo va dedicado para todos ustedes con un profundo agradecimiento.

AGRADECIMIENTO

Quiero expresar mi agradecimiento a mis padres, abuelos, hermano, amigos por estar siempre presentes en esta etapa importante de mi vida. Su apoyo incondicional y compañía han sido los pilares fundamentales para culminar con éxito mi camino universitario

RESUMEN

El presente trabajo de investigación titulado "Análisis de las Vulnerabilidades y Mitigación de Riesgos relacionados con la seguridad de la información en la empresa Urban Lab Effect S.A.S", se ha llevado a cabo con el objetivo de evaluar y abordar los desafíos de seguridad de la información en la mencionada empresa, tomando como referencia las normativas ISO 27001 y 27002.

En primer lugar, se realizó un análisis exhaustivo de la empresa en términos de seguridad de la información, examinando detalladamente los procedimientos, procesos y políticas existentes. Este análisis permitió identificar las áreas vulnerables y los riesgos asociados a la seguridad de la información en la organización.

Con base en los hallazgos obtenidos, se ha desarrollado un plan de acción estratégico base que establece las medidas y procedimientos claves y necesarias para fortalecer la seguridad de la información, alineadas con los estándares internacionales. Este plan de acción proporciona una guía clara para que la organización implemente las mejoras necesarias, adaptándolas según su criterio y disponibilidad de recursos.

Para obtener una visión más precisa de la situación, se llevaron a cabo conversaciones con dos líderes de área de la organización. Estas charlas fueron de gran relevancia, ya que permitieron concluir que la seguridad de la información en la empresa era prácticamente inexistente en la mayoría de los escenarios. Este hallazgo representa un riesgo significativo para la empresa, ya que la seguridad de la información es fundamental para salvaguardar los activos y la confianza de los clientes.

En resumen, este trabajo de investigación ha abordado el análisis de las vulnerabilidades y la mitigación de los riesgos asociados con la seguridad de la información en la empresa Urban Lab Effect S.A.S. Se ha realizado un análisis exhaustivo de la organización, se ha desarrollado un plan de acción alineado con las normativas internacionales y se ha evidenciado la necesidad urgente de mejorar la seguridad de la información dentro de la empresa. La implementación de este plan contribuirá a proteger los activos y fortalecer la confianza tanto interna como externa en la organización.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I: INTRODUCCIÓN

1. Marco de Referencia

1.1. Justificación

De acuerdo con un informe del International Data Corporation (2021), se proyecta que para el año 2025, una persona promedio se conectará a la red aproximadamente 4800 veces al día a través de una variedad de dispositivos, lo que les permitirá intercambiar información con otros individuos.

En los tiempos modernos, los datos se consideran el recurso más valioso a nivel mundial debido a su capacidad para ofrecer un amplio conocimiento en áreas como comportamientos, identificaciones, estadísticas y toma de decisiones, entre otros aspectos. Por esta razón, es crucial y vital proteger este tipo de recurso utilizando todas las metodologías y herramientas disponibles para optimizar y resguardar la información empresarial ante las múltiples amenazas del entorno externo.

Por tal razón se propone el presente tema de titulación para realizar un análisis de vulnerabilidades y una propuesta de mitigación de riesgos relacionados a la seguridad de la información que tiene la empresa Urban Lab Effect S.A.S., tomando como referencia los lineamientos establecidos dentro de la norma ISO 27001 y 27002.

1.2. Planteamiento del problema

En los últimos años, la empresa Urban Lab Effect S.A.S. ha experimentado un notable crecimiento en el mercado nacional e internacional, lo que la ha llevado a posicionarse como una de las empresas más conocidas en el campo educativo y tecnológico, debido a su amplia cartera de clientes en el Ecuador. El crecimiento de la empresa ha implicado la incorporación de nuevas herramientas, servicios de terceros y otros insumos que trabajan directamente con los datos y

sistemas de la empresa. No obstante, dicho crecimiento también implica un incremento en el peligro de posibles riesgos y amenazas que afecten la integridad y seguridad de la información empresarial. Entre las amenazas más comunes se encuentran el malware, las amenazas internas, los ataques de phishing, los desastres naturales, los fallos del sistema y los ataques externos. Todos estos ataques representan un riesgo para la empresa, por lo que se ha optado por una revisión de los riesgos relacionados a la seguridad de la información y como prevenirlos mediante la emisión de una hoja de ruta, que abarcará aspectos clave como la evaluación de riesgos, implantación y elaboración de políticas de seguridad, capacitación y concientización de los colaboradores y la implementación de planes de respuesta a incidentes, que servirá como una línea base para la empresa y poder mejorar su situación con la seguridad de la información.

1.2.1. Objetivo General

Evaluar las vulnerabilidades y los riesgos relacionados a la seguridad de la información en la empresa Urban Lab Effect S.A.S, tomando como referencia las normas ISO 27001 y 27002.

1.2.2. Objetivos Específicos

1. Fundamentar los parámetros exigidos por las normas ISO 27001 y 27002 relacionados a la gestión de la seguridad de la información.
2. Analizar el nivel de la seguridad de la información en la empresa, tomando en cuenta los estándares establecidos en las normas ISO 27001 y 27002.
3. Evaluar las políticas y prácticas de seguridad de la información de la empresa, incluyendo el uso de contraseñas seguras, la encriptación de datos y el acceso restringido a la información confidencial.
4. Establecer un plan de acción guiado por las normas ISO 27001 y 27002 para la minimización de riesgos en la empresa Urban Lab Effect S.A.S.

1.3. Antecedentes

Los antecedentes del presente trabajo de titulación tienen como foco principal el análisis y la mitigación de los riesgos relacionados a la seguridad de la información en la empresa Urban Lab Effect S.A.S. Durante los últimos diez años, en Ecuador, los ataques cibernéticos han aumentado de manera continua y se han dirigido a empresas de diversos tamaños y sectores. Esta situación ha puesto en riesgo la confidencialidad, integridad y seguridad de la información. Por tanto, este trabajo tiene como objetivo llevar a cabo un análisis parametrizado dentro de la empresa con el fin de tomar las medidas proactivas necesarias para prevenir y mitigar todos los posibles riesgos de seguridad de la información, garantizando así la continuidad de sus operaciones mediante un plan de acción estratégico.

1.4. Alcance

El alcance de este trabajo en la empresa Urban Lab Effect S.A.S será detallado, con el objetivo principal de evaluar y mejorar la seguridad de la información de la organización. El análisis cubrirá una revisión del sistema principal de la empresa, evaluando sus potenciales y riesgos y vulnerabilidades. Además, se evaluarán las políticas y prácticas de seguridad de la información de la empresa, tomando como base la normativa ISO 27001:2013. Al concluir, se elaborará un plan de acción detallado con los resultados de la evaluación, las recomendaciones y medidas propuestas para fortalecer la seguridad de la información de la empresa. Con este alcance, se espera que el análisis realizado ayude a la empresa a mejorar sus niveles de seguridad de la información y de esta manera proteger sus activos digitales de posibles amenazas y riesgos eventuales que se puedan llegar a presentar.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2. Marco Teórico

2.1. Seguridad de la Información.

2.1.1. Concepto y definición de la Seguridad de la Información.

Cuando se menciona la seguridad de la información, se hace referencia al conjunto de medidas y técnicas empleadas para proteger, supervisar y asegurar todos los datos y la información gestionada en el ámbito empresarial. El objetivo primordial de la seguridad de la información radica en garantizar la integridad, confidencialidad y disponibilidad de la información, los cuales son los tres elementos fundamentales para considerar un sistema seguro, tal como se muestra en la representación visual denominada Figura 1. Dicha ilustración presenta los tres pilares esenciales conocidos como los fundamentos de la seguridad de la información.

Figura 1 Pilares de la Seguridad de la Información. Fuente: (Sánchez, 2007)

El primer pilar, la confidencialidad, se enfoca en la salvaguardia y protección de la información frente a accesos no autorizados. En otras palabras, un sistema seguro debe asegurar que solo las personas autorizadas, aquellas con los permisos correspondientes, puedan acceder a la información protegida de la organización. Para lograr esto, se emplean diversas técnicas de seguridad que se describirán posteriormente.

El segundo pilar, la integridad, se centra en la protección de la información frente a las anomalías o alteraciones no identificadas o sospechosas que intenten atacar a la empresa.

Además de la confidencialidad, un sistema seguro debe garantizar que la información no pueda ser modificada o extraída por personas sin autorización.

Finalmente, el tercer pilar, conocido como disponibilidad, asegura que tanto el sistema como toda la información contenida en él estén accesibles y disponibles cuando se necesiten. Este último aspecto es vital para el correcto funcionamiento de cualquier organización puesto que un sistema seguro debe estar diseñado para resistir ataques que puedan afectar su disponibilidad (Toro, 2021).

2.1.2. Importancia de la seguridad de la información.

Como se mencionó anteriormente, la protección de la información se ha convertido en un tema de suma importancia y actualidad para las organizaciones en todos los sectores y tamaños a nivel global. Esto se debe al aumento de las amenazas y ataques cibernéticos que han afectado a diversas empresas a nivel nacional e internacional. Por ende, es crucial que las empresas implementen las medidas necesarias para asegurar la protección de su información.

> “Entre los principales puntos que busca proteger y resguardar la seguridad de la información está la protección de los datos personales, la prevención de la pérdida de la información crítica de la empresa y la continuidad del negocio” InfoCDMX (s.f).

Por esta razón, es vital asegurar estos datos mediante ciertos mecanismos, puesto que representan información personal valiosa que puede revelar detalles privados y confidenciales.

Según la información encontrada en el sitio web de Proofpoint (s.f.), la prevención de la pérdida de información crítica es fundamental para la estabilidad y continuidad de la empresa. Una potencial pérdida de esta información podría tener consecuencias financieras negativas, así como comprometer la reputación de la empresa y llevar a la pérdida de clientes que desembocaría en la desaparición de la empresa. Además, en algunos casos, las empresas pueden estar sujetas a multas gubernamentales, como en Ecuador y la Ley Orgánica de

Protección de Datos, por no proteger adecuadamente la información crítica manejada dentro de la organización. Por lo tanto, es esencial implementar medidas de protección adecuadas como el uso de programas de Data Loss Prevention (DLPs), sensibilizar y concientizar al personal y establecer e implementar políticas y procedimientos organizacionales relacionados y alineados a la seguridad de la información.

La protección de la continuidad empresarial frente a las amenazas cibernéticas es un elemento esencial en el ámbito de la seguridad de la información. Este aspecto se refiere a todos los actores malintencionados que buscan interrumpir las operaciones de las empresas y causar un impacto económico considerable, como la pérdida o sustracción de datos, interrupción de los sistemas o distribución de software malicioso con el objetivo de atacar a la organización (Kaspersky, s.f.).

Por lo tanto, en los tiempos modernos es importante contar con medidas preventivas para evitar este tipo de amenazas y garantizar la continuidad del negocio ante cualquier situación potencial de riesgo, tal como se mencionó anteriormente.

2.1.3. Ley Orgánica de Protección de Datos Personales en el Ecuador

De acuerdo con la “Ley Orgánica de Protección de Datos Personales” proporcionada por la Asamblea Nacional del Ecuador (2021), establece los principios, derechos y obligaciones relacionados con la recopilación, uso, almacenamiento y transferencia de datos personales en Ecuador. El propósito de esta legislación es salvaguardar la privacidad y garantizar el adecuado manejo de la información personal de los individuos, estableciendo mecanismos y medidas de protección para su correcto tratamiento. La ley fue promulgada el 27 de mayo de 2021 y se encuentra en vigor desde esa fecha, estableciendo diversas obligaciones legales para la protección de datos personales en el país. Además, se han definido algunos parámetros generales que las empresas deben cumplir para su implementación, como la sensibilización y capacitación, el análisis de riesgos y evaluación de su impacto, la implementación de medidas

de seguridad de la información y la designación y conformación de un equipo responsable para la protección de datos.

2.2. Amenazas más comunes en el Ecuador

"Las últimas tendencias en el Ecuador han llevado a un aumento creciente de las amenazas cibernéticas en estos últimos años. El aumento de los dispositivos electrónicos, el avance de las tecnologías de la información y comunicación y el aumento de la conectividad han dado lugar a nuevas formas de ataques cibernéticos que ponen en riesgo la seguridad y la privacidad de las empresas y los ciudadanos del país" (Onofa, 2022).

Además, según Mercedes Onofa (2022), "Ecuador se suma a Argentina, Brasil, Colombia, México y Perú, como uno de los países de Latinoamérica más golpeados por los delitos informáticos, principalmente códigos maliciosos (malware)".

2.2.1. Contexto de la situación en el Ecuador

Según un estudio realizado, el Ecuador ocupa el quinto lugar en cuanto a ataques de phishing en América Latina. El phishing es una de las técnicas de estafas o ataques más comunes en todo el mundo, y que emplea ciertas técnicas de ingeniería social para engañar a la víctima. Además, entre las amenazas de seguridad más comunes a nivel nacional se encuentran los ataques de phishing, malware, ataques de ransomware, ataques de denegación de servicios (DDoS) y ataques de ingeniería social. En este último y más reciente tipo de técnica, el atacante busca establecer comunicación con su objetivo con el fin de persuadir y engañar a la víctima mediante correos engañosos (spam), llamadas y otros métodos con el fin de vulnerar la seguridad de la persona o usuario. (Guaña-Moya et al, 2022).

2.2.2. Ransomware

"El ransomware es uno de los ataques que están actualmente en tendencia en todo el mundo y que también acecha a Ecuador" (FortiGuard Labs, 2022).

Ya se han reportado casos dentro del país sobre esta modalidad de ataque, como los casos del Banco Pichincha y la Corporación Nacional de Telecomunicaciones (CNT) ocurridos en el año 2021, donde dichos ataques perjudicaron negativamente la reputación de las empresas mencionadas, inhabilitaron sus servicios y afectaron directamente a todos sus clientes.

Tal y como lo menciona Kaspersky (2023), el ransomware es una clase de malware extorsivo que tiene como finalidad secuestrar información vital de una organización para cobrar un rescate.

2.2.3. Smishing

Según el paper titulado "Ataques de phishing y cómo prevenirlos" (Guaña-Moya, J., Jaramillo-Flores, P. C., Mora-Zambrano, E. R., Chiluisa-Chiluisa, M., Naranjo-Villota, D., & Larrea-Torres, L. G., 2022), el smishing es una forma de ataque cada vez más común en Ecuador y en otros lugares del mundo. Este ataque consiste en el envío de mensajes de texto maliciosos a los usuarios de teléfonos móviles, con el único propósito de engañarlos y extraer su información confidencial. Estos mensajes suelen parecer legítimos y pueden contener enlaces a sitios web fraudulentos o solicitar datos personales. En este tipo de ataque, los delincuentes utilizan tácticas de ingeniería social para aprovechar la confianza de las personas y persuadirlas de que compartan su información sensible, como registros de sesión y contraseñas, números de tarjetas de crédito o números del seguro social.

2.2.4. Vishing

El vishing, también conocido como suplantación telefónica, es una forma de ataque que ha ganado popularidad en Ecuador (Guaña-Moya et al, 2022). En este tipo de estafa, los delincuentes realizan llamadas telefónicas haciéndose pasar por personas o entidades de confianza, como instituciones financieras o empresas reconocidas. Mediante técnicas de manipulación psicológica, buscan obtener información sensible o convencer a las víctimas de que realicen determinadas acciones perjudiciales. Es crucial que los individuos estén alertas y

desconfíen de las llamadas telefónicas inesperadas que soliciten información personal o financiera, a fin de protegerse contra el vishing y salvaguardar su seguridad.

2.2.5. Pharming

El pharming es otra forma de ataque cibernético que ha sido documentada en la investigación de Guaña-Moya et al. (2022). En este tipo de ataque, los delincuentes cibernéticos manipulan el Sistema de Nombres de Dominio (DNS) con el objetivo de redirigir a los usuarios a sitios web fraudulentos sin su conocimiento. Estos sitios web fraudulentos están diseñados para parecer legítimos y pueden solicitar la información confidencial, como contraseñas, números de tarjetas de crédito, números de contacto y direcciones domiciliarias. Es fundamental que los usuarios estén conscientes de este tipo de amenaza y tomen medidas para protegerse, como verificar la autenticidad de los sitios web y utilizar conexiones seguras.

2.2.6. Ataques de Denegación de Servicios

Otra de las formas de ataque que se observan frecuentemente en el ámbito nacional es el ataque de denegación de servicios (DDoS). Este ataque consiste en vulnerar un servidor u ordenador desde muchos equipos en simultáneo. Esta avalancha de datos ocasiona que los recursos del servidor colapsen, provocando un fallo inminente y que su funcionamiento sea nulo. Esto hace que todas las personas caigan junto al servidor y afectando las operaciones de la empresa. (Xataka, 2022).

Por último, uno de los casos más recientes de ataques relacionados a la denegación de servicios, fue en el pasado mes de marzo del presente año donde el medio comunitario “Wambra”, comunicó que sufrió un ataque DDoS que lo dejó fuera del aire durante 5 horas y las personas no pudieron acceder al sitio en ese periodo de tiempo, lo que generó un impacto negativo en la reputación del medio informativo local y en sus operaciones.

2.3. Medidas de seguridad de la información.

Las amenazas cibernéticas están aumentando en frecuencia dentro del entorno empresarial y su objetivo principal es afectar a las organizaciones mediante el acceso no autorizado a sus activos y su compromiso. En este sentido, la protección de la privacidad de los datos se ha vuelto crucial para todas las empresas, asegurando así la confidencialidad, integridad y disponibilidad de la información. En la actualidad, se implementan diversas medidas de seguridad de la información en la mayoría de las organizaciones con el fin de mitigar los riesgos, como la protección de datos, la autenticación de usuarios, la actualización de software, la capacitación y concientización del personal, entre otras.

2.3.1. Protección de datos

Esta medida de seguridad de la información tiene como eje principal la protección de los datos financieros, personales y administrativos de una empresa para evitar el acceso no autorizado a este tipo de activo crucial. Entre las medidas más comunes de la protección de datos se encuentra el cifrado, la implantación de políticas sobre la gestión de la información empresarial, realización de copias de seguridad y la implementación de sistemas de antivirus que permitan identificar posibles amenazas y prevenirlas.

2.3.2. Autenticación de usuarios

La verificación de la identidad de los usuarios es una medida adicional en la seguridad de la información que tiene como objetivo autenticar y confirmar la identidad de los usuarios, proporcionando así un método seguro de acceso para los usuarios de la empresa. Esto se logra mediante la implementación de autenticación de dos factores, el uso de contraseñas seguras y la aplicación de autenticación biométrica, lo cual ayuda a prevenir el acceso no autorizado de personas externas a la organización a la información confidencial (Bowen, Hash, Wilson, 2006).

2.3.3. Encriptación de datos

La encriptación de datos es otra medida crucial para salvaguardar la confidencialidad de la información durante su almacenamiento, transmisión y procesamiento. Su objetivo es transformar los datos en un formato ilegible utilizando algoritmos criptográficos, de modo que solo las personas autorizadas que posean la clave correcta puedan descifrarlos y acceder a su contenido original.

La encriptación se puede aplicar tanto a nivel de dispositivos como a nivel de redes y comunicaciones. Por ejemplo, en dispositivos como computadoras o dispositivos móviles, se puede implementar la encriptación de disco completo para proteger todos los datos almacenados en el dispositivo. De esta manera, en caso de pérdida o robo del dispositivo, los datos no pueden ser accesibles sin la clave de encriptación correspondiente.

2.3.4. Respaldo y recuperación de los datos

Según el artículo "Respaldo y recuperación de base de datos" (Serman, 2023), es importante implementar estrategias adecuadas de respaldo y recuperación de las bases de datos empresariales para garantizar la seguridad y la continuidad del negocio.

Es por tal razón que el respaldo y la recuperación de datos son medidas esenciales en este campo, ya que garantizan la disponibilidad y la integridad de los datos de la organización en caso de eventos adversos, como fallas técnicas, desastres naturales o ataques cibernéticos.

El respaldo de datos consiste en realizar copias de seguridad periódicas de la información catalogada como importante de la empresa y almacenarlas en ubicaciones seguras, tanto físicas como en la nube. La recuperación de datos, por su parte, se refiere a la capacidad de restaurar dichos datos respaldados en caso de que se produzca un evento adverso como la pérdida o algún incidente que afecte la disponibilidad de la información.

Estas medidas son fundamentales para garantizar la continuidad del negocio y minimizar el mayor grado de impacto de un posible incidente.

2.4. ISO 27001

2.4.1. ¿Qué es la norma ISO 27001?

Según GlobalSuite Solutions (s.f.), la normativa ISO 27001 es un estándar internacional creado por el Organismo Internacional de Estandarización (ISO), que establece todas las bases para la correcta implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización. Esta norma tiene como objetivo ayudar a todas las organizaciones a establecer, mejorar e implementar el SGSI.

2.4.2. Importancia

Esta norma es considerada una de las herramientas y mecanismos más importantes en una organización puesto que busca garantizar la correcta preservación de su información y pretende mitigar todos los riesgos relacionados a la seguridad de la información en la organización.

Por otro lado, esta normativa internacional también ofrece un panorama completo sobre la correcta gestión de la seguridad de la información y como una organización debe cumplir con todos los requisitos legales para poder acceder a esta certificación.

La certificación mencionada ha adquirido una reputación destacada como una de las normas de seguridad de la información más reconocidas y respetadas a nivel global en la actualidad. Es ampliamente adoptada por organizaciones de diversos sectores en todo el mundo.

2.4.3. Fortalezas

La norma ISO 27001 presenta diversas ventajas significativas en el ámbito de la seguridad de la información. Según PMG SSI (2016), esta norma se distingue por su capacidad para proteger activos valiosos, como la información de clientes y empleados. Además, su enfoque centrado en

los procesos, en consonancia con el Sistema de Gestión de Seguridad de la Información (SGSI), asegura la implementación de controles eficaces. Entre los puntos fuertes más destacados de la norma se incluyen:

- La protección de todos sus activos como la información de los clientes y empleados.
- Posee un enfoque basado en procesos alineados al Sistema de Gestión de Seguridad de la Información (SGSI).
- Otorga un certificado de confianza y calidad empresarial.
- Está enfocado en la correcta gestión de riesgos relacionados a la seguridad de la información.
- Es reconocida de manera internacional y representa un gran compromiso con la seguridad de la información.

2.4.4. Debilidades

En cuanto a las debilidades, se puede destacar que en ciertas ocasiones la norma puede ser compleja y su implementación puede representar un costo muy alto. Además, esta norma se encuentra en un cambio constante (PMG SSI, 2016).

Entre las principales debilidades se encuentran:

- En ciertas ocasiones, puede llegar a ser compleja de comprender para la organización y sus colaboradores.
- Su implementación puede llegar a ser muy costosa dependiendo el tamaño de la organización.
- La norma ISO 27001 se encuentra constantemente en cambios para mantenerse al día con las nuevas amenazas de seguridad.

2.5. ISO 27002

2.5.1. ¿Qué es la norma ISO 27002?

El estándar internacional ISO 27002 es un conjunto de directrices y mejoras ampliamente reconocido en el campo de la seguridad de la información. Esta norma fue lanzada en 2005 y se actualizó en 2013.

Según ISO (2020), este estándar se enfoca en garantizar la seguridad de la información y establece un marco de referencia para las políticas y procedimientos de seguridad, así como para la gestión de riesgos, incidentes y otros aspectos relevantes.

2.5.2. Importancia

"Esta norma internacional es de vital importancia dentro de las organizaciones a nivel mundial, ya que permite conocer de manera exacta y objetiva todos los activos que posee una empresa, como los recursos de información, recursos de software, activos físicos, servicios y otros más" (NQA, s.f.). Además, proporciona recomendaciones y buenas prácticas para la gestión de la seguridad de la información en la organización. Como se mencionó previamente, esta norma establece un marco de referencia para la implementación de medidas de seguridad de la información (NQA, s.f.).

2.5.3. Fortalezas

La norma ISO 27002 es una guía completa y detallada para la gestión de la seguridad de la información en las organizaciones. Además, proporciona un medio para que las empresas cumplan con los requisitos legales relacionados con la seguridad de la información y se adapten al marco legislativo de cada país. Al implementar esta norma internacional, las organizaciones pueden identificar y gestionar de manera eficiente los riesgos de seguridad de la información, garantizando la protección y confidencialidad de sus activos más valiosos. Según ISO (2020), la norma ISO 27002 ofrece un marco de referencia para las políticas y procedimientos de seguridad, así como para la gestión de riesgos, incidentes y otros aspectos relacionados.

Entre las principales ventajas de esta norma se encuentran:

- La efectividad de la gestión de la seguridad de la información no está garantizada por esta norma, ya que dependerá de cómo la organización implemente los controles y prácticas recomendadas.
- A diferencia de la ISO 27001, esta norma no se actualiza regularmente, lo que impide que las organizaciones estén al tanto de los últimos riesgos y amenazas en el ámbito de la seguridad de la información.
- La implementación de esta norma puede tener repercusiones económicas negativas dentro de una organización, ya que puede requerir una inversión significativa y la participación de múltiples partes interesadas en la empresa.

2.5.4. Debilidades

Según Toro (2021), la norma ISO 27002 proporciona una variedad de controles y prácticas recomendadas eficaces para la gestión adecuada de la seguridad de la información en las organizaciones. No obstante, es relevante considerar que la efectividad de estos controles y prácticas depende de cómo la organización los implemente.

Algunas de las limitaciones más destacadas de esta norma incluyen:

- Esta norma no garantiza la efectividad completa de la gestión de la seguridad de la información, puesto que dependerá de cómo la organización implemente los controles y las prácticas recomendadas de manera interna.
- A diferencia de la ISO 27001, esta norma no se actualiza constantemente por lo que no mantiene al día a las organizaciones con respecto a los últimos riesgos y amenazas de la seguridad de la información.

- La implementación de esta norma puede tener un impacto negativo en lo económico dentro de una organización puesto que puede requerir una inversión significativa y requiere la participación de varias partes dentro de la empresa.

CAPÍTULO III: METODOLOGÍA

3. Metodología

3.1. Descripción de la muestra

3.1.1. Empleados de Urban Lab Effect S.A.S

La muestra seleccionada se limitará exclusivamente a los jefes de área de finanzas y TI de Urban Lab Effect S.A.S. Esto se debe a que estos líderes desempeñan un papel crucial en las operaciones diarias y en la protección de la información. Al incluir únicamente a estos jefes de área, se obtendrá una visión más panorámica de los niveles actuales de seguridad de la información en la empresa.

3.1.2. Área de TI

La muestra seleccionada incluirá al jefe de área de tecnología y al personal encargado de la seguridad de la información en la empresa. Dado que el área de tecnología desempeña un rol fundamental en la implementación y supervisión de las medidas de seguridad, se considera crucial su participación en la muestra. De esta manera, se obtendrá una visión más completa y precisa de los niveles de seguridad de la información en la empresa.

3.1.3. Criterios de la selección

La selección de la muestra en esta investigación es un paso primordial para garantizar la validez de los resultados y de los participantes. A continuación, se presentan los diversos criterios que se utilizarán en la investigación.

- Ser empleado activo de Urban Lab Effect S.A.S
- Tener experiencia en el manejo de la información empresarial.
- Pertenecer a un área específica dentro de la empresa.

3.2. Tipo de investigación

3.2.1. Enfoque de la investigación

Para este análisis, se ha optado por el enfoque de investigación exploratoria. Esta elección de enfoque se basa en la relevancia de la información y en el reciente crecimiento del campo de la seguridad de la información en la organización, especialmente con relación a la Ley Orgánica de Protección de Datos (LOPD). La investigación exploratoria nos permitirá adentrarnos en este tema emergente y obtener una comprensión más profunda de los desafíos, implicaciones y panorama dentro de la empresa.

3.3. Metodología escogida

3.3.1. Descripción de la metodología

La metodología que utilizaremos para el desarrollo de esta investigación se fundamentará en la normativa ISO 27001:2013. Esta norma ofrece un enfoque integral para analizar las vulnerabilidades asociadas a la seguridad de la información dentro de la empresa seleccionada.

3.3.2. Objetivos principales de la metodología

- Identificar las vulnerabilidades relacionadas a la seguridad de la información en la empresa Urban Lab Effect S.A.S.
- Evaluar las prácticas actuales de la gestión de seguridad de la información en la empresa Urban Lab Effect S.A.S.
- Desarrollar un plan de acción para mitigar las vulnerabilidades identificadas y proponer una mejora en la gestión de la seguridad de la información dentro de la empresa Urban Lab Effect S.A.S.

3.4. Variables

En el contexto relacionado a esta investigación, se han identificado múltiples variables que van a ser consideradas para el correcto análisis de la seguridad de la información dentro

de Urban Lab Effect S.A.S. Cabe mencionar que cada una de las variables son importantes y tienen un nivel de impacto alto en la seguridad de la información de la empresa. Entre las variables que se analizarán están las siguientes y como se medirán.

- Tamaño de la empresa: Se evaluará el tamaño de la empresa.
- Infraestructura tecnológica: Se evaluará e identificará la infraestructura tecnológica utilizada en la empresa. (referirse al Anexo C)
- Políticas de seguridad: Se analizarán las políticas y los procedimientos establecidos por la empresa. (referirse al Anexo B)
- Evaluación de las vulnerabilidades: Se analizarán las herramientas utilizadas para la mitigación de vulnerabilidades. (referirse al Anexo C)
- Cumplimiento normativo con la legislación ecuatoriana: Se evaluará si la empresa cumple con la normativas y regulaciones relacionadas con la Ley Orgánica de Protección de Datos Personales. (LOPD)

3.5. Instrumentos de recolección de datos

3.5.1. Conversaciones

Se charló de manera directa con dos jefes de distintas áreas específicas de la empresa. Estas charlas tuvieron como objetivo conocer a la empresa, su jerarquía, estado actual, políticas y procedimientos. Se hicieron preguntas puntuales sobre la organización para conocer el panorama completo de la seguridad de la información.

3.5.2. Observaciones

Con relación a la recopilación de datos, se llevaron a cabo entrevistas directas con dos responsables de diferentes áreas específicas de la empresa como método de obtención de información. Estas entrevistas tenían como objetivo principal adquirir un conocimiento detallado de la estructura organizativa, la situación actual de la empresa y sus políticas y procedimientos

relacionados con la seguridad de la información. Durante las entrevistas se formularon preguntas específicas con el fin de obtener una visión integral del panorama de la seguridad de la información en la organización.

3.5.3. Matriz de consideraciones basada en la norma ISO 27000

Se utilizó una matriz (referirse al Anexo A) de consideraciones como guía para conocer y evaluar el verdadero estado actual de la empresa con respecto a los lineamientos de la norma ISO 27000. Esta matriz incluye los elementos importantes con respecto a la normativa internacional.

3.6. Procedimiento de recolección de datos

3.6.1. Charlas con los jefes

Se realizó una serie de preguntas relacionadas a la seguridad de la información de la empresa con los distintos jefes de áreas (Tecnología y Financiero). Se formularon preguntas puntuales y estructuradas sobre los parámetros de la seguridad de la información y las buenas prácticas en la empresa y se registraron detalladamente las respuestas de los participantes, respetando un acuerdo verbal de confidencialidad y privacidad. (referirse al Anexo A)

3.6.2. Realización de observaciones

Estas observaciones se realizaron en diferentes áreas de la empresa, donde se recopiló información visual sobre las prácticas de seguridad de la información, se registraron los hallazgos relevantes y otros aspectos relacionados a los parámetros de seguridad.

Además, se utilizaron fotografías para documentar algunas de las observaciones de una manera más objetiva. (referirse al Anexo E).

3.6.3. Recopilación de los datos

Una vez finalizado el proceso de recolección de datos, se procedió a recopilar toda la información de manera escrita en las matrices de la situación actual de la empresa para el

posterior análisis. Además, se organizaron las observaciones realizadas para llevar a cabo la investigación manteniendo la confidencialidad de la información recopilada mediante la supresión de los nombres de los distintos jefes de la organización.

3.7. Proceso de análisis de datos

3.7.1. Organización de los datos

Se ejecutó una organización de manera ordenada de todos los datos recolectados, tanto de las charlas como de las observaciones realizadas. Esto implicó escribir las respuestas de los involucrados con relación a la situación actual de la empresa en la matriz planteada. (referirse al Anexo A).

3.7.2. Comparación con la matriz

Se empleó la matriz de las consideraciones basada en la normativa ISO 27001 como un marco de referencia para la evaluación de los parámetros de la seguridad de la información.

3.8. Consideraciones éticas

3.8.1. Privacidad

Se acordó con uno de los representantes de la empresa no divulgar los procedimientos internos que son considerados confidenciales y que podrían afectar a la competitividad de la empresa. Además, se acordó mantener el anonimato de todos los colaboradores de la organización y no revelar datos cruciales de la organización mediante un acuerdo de confidencialidad y privacidad. (referirse al Anexo D).

3.8.2. Consentimiento

Se obtuvo el consentimiento previo de los participantes involucrados en esta investigación y se brindó una explicación clara y concisa sobre el propósito de la investigación.

3.8.3. Cumplimiento de normas éticas

Se consideraron todos los principios éticos para garantizar la validez y la fiabilidad de los datos recopilados y se revisaron las normativas legales y regulaciones establecidas por la Legislación Ecuatoriana en relación con la Ley Orgánica de Protección de Datos Personales (LOPD).

CAPÍTULO IV: DESARROLLO DE LA INVESTIGACIÓN

4.1. Descripción de la empresa

Urban Lab Effects S.A.S es una empresa establecida en Quito, Ecuador. Fue fundada en el año 2015 y se dedica a la industria del Diseño de Sistemas Informáticos y Servicios Relacionados. La empresa se especializa en ofrecer distintas soluciones en el campo del desarrollo web y móvil mediante la creación de sitios web dinámicos y fluidos, así como aplicaciones móviles innovadoras.

4.2. Organigrama de la empresa

En la Figura 2 se visualiza como está distribuida la organización dentro la empresa.

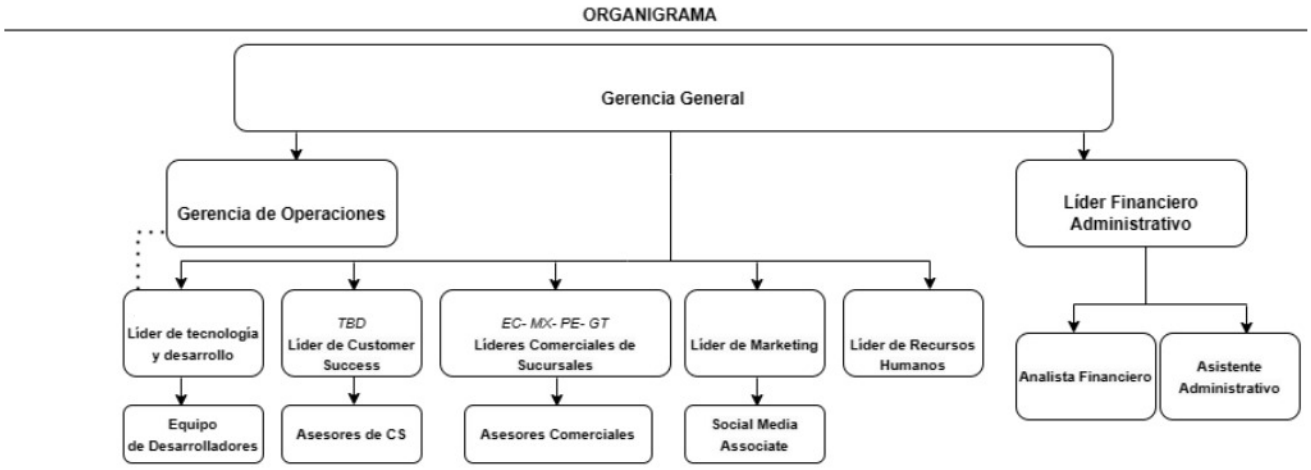


Figura 2 Organigrama de Urban Lab Effect S.A.S

4.3. Misión y valores de la empresa

Misión

- Transformamos el mundo de la educación.

Valores

- Optimismo
- Trabajo en equipo
- Compromiso

- Enfoque en el usuario

4.4. Situación de la empresa relacionado a la seguridad de la información

La empresa Urban Lab Effects S.A.S actualmente cuenta con ciertos parámetros establecidos que tienen como objetivo mitigar los potenciales riesgos en la organización, sin embargo, estos no están alineados con los conceptos básicos sobre la gestión de la seguridad de la información y como se establecen en los lineamientos de la norma ISO 27001.

4.5. Activos

Un activo de la información hace referencia a todo tipo de información y datos que tienen un nivel de valoración que requiere protección para asegurar su confidencialidad, integridad y disponibilidad. Estos activos son considerados vitales para la organización ya que pueden incluir información financiera, datos, personales, acuerdos, documentación de propiedad intelectual y otros.

Es por tal razón, que se deben implementar las medidas de seguridad adecuadas para resguardarlas como es el uso de firewalls, políticas internas, criptografía y demás controles que pueden estar regulados por normativas internacionales como la ISO 27001.

4.5.1. Categoría de los activos

En la Tabla 1 se muestra cómo van a estar distribuidas las categorías de la clasificación de los activos alineándose al marco establecido dentro de la norma ISO 27001.

Tabla 1 Clasificación de los Activos de la Información.

Activos de Información	Se refiere a todos los documentos, manuales y acuerdos que contienen información valiosa de la empresa.

Activos de Software	Se refiere a todos los programas, programas de propiedad intelectual y sistemas operativos utilizados dentro de la empresa.
Activos de Hardware	Se refiere a todos los equipos físicos utilizados en la empresa como computadores de escritorios, laptops, celulares, tablets, entre otros.
Activos de Red	Se refiere a toda la infraestructura de red incluyendo los dispositivos de red que son utilizados para la comunicación dentro de la empresa.

4.5.2. Tipos de activos

Según los anexos (A.8.2, A.8.3, A.8.4) establecidos dentro la normativa internacional ISO 27001, los activos de la información pueden ser catalogados de la siguiente manera como se muestra en la Tabla 2.

Tabla 2 Tipos de Activos de la Información

Tipo de activo	Descripción
Activos de Información	Se trata de toda la información que esté relacionada a la empresa como acuerdos, documentación, acuerdos, entre otros.
Activos de Software	Se trata de todos los sistemas que estén asociados a la empresa y en sus funciones como licencias, software propio, entre otros.
Activos de Hardware	Se trata de todos los equipos que estén relacionados directamente con la organización como PCs, laptops, tablets, celulares, entre otros.
Activos de Red	Se trata de los equipos de red que estén relacionados directamente con el funcionamiento de la organización como routers, Access Points, servidores, firewalls, entre otros.

4.5.3. Clasificación de la información

En la Tabla 3, se muestra el tipo de información según el nivel de acceso que la empresa debe establecer para la clasificación de su información.

Tabla 3 Clasificación de la Información

Público	Información que se encuentra publicada y es de libre acceso.
Uso Interno	Información de uso interno que solo podrá ser divulgada a terceros previa autorización.
Restringido	Información que requiere una autorización otorgada por el jefe de la organización.
Confidencial	Información que se encuentra disponible únicamente para la empresa.

4.5.4. Matriz de activos de la organización

Esta matriz representa una herramienta principal y estratégica que permite identificar, categorizar y evaluar todos los activos fundamentales de la empresa, con el objetivo de conocer el valor, nivel de vulnerabilidad y los principales riesgos asociados a ellos. Además, según la norma ISO 27001 esta matriz proporciona una hoja de ruta para establecer una correcta gestión de la seguridad de la información en la organización. En la Tabla 4 se visualizan los activos claves implicados en las operaciones diarias de la organización.

Tabla 4 Matriz de activos de la Empresa.

Nombre del activo	Tipo	Descripción	Tipo de Información	Criticidad	Riesgos Identificados
Core de Idukay	Software	Software utilizado para las operaciones de la empresa.	Confidencial	Alto	Interrupción del servicio.
Manuales Core	Información		Confidencial	Alto	

		Documentación y manuales relacionado al Core de la empresa.			Divulgación no autorizada, pérdida de información.
Bases de datos Idukay	Software	Base de datos utilizadas para las operaciones de la empresa.	Confidencial	Alto	Fuga de información.
Información de clientes	Información	Datos personales de todos los clientes almacenados en las bases de datos y sistemas internos de la empresa.	Confidencial	Alto	Divulgación no autorizada, acceso indebido a los datos de los clientes.
Equipos	Hardware	Equipos portátiles, PCs, laptops, celulares de la empresa.	Uso interno	Medio	Robo, pérdida, accidentes.
Servidores	Hardware	Servidores físicos y virtuales utilizados para las funciones de la empresa.	Uso interno	Medio	Acceso no autorizado
Router	Red	Dispositivo que controla el tráfico de red de la empresa.	Público	Bajo	Interrupción de la conectividad.
Firewall	Red	Dispositivo que controla el tráfico de red de la empresa.	Público	Bajo	Ataques de Red.

4.6. Observación de deficiencias de seguridad en la empresa

4.6.1. Propósito de la observación

El propósito de esta observación consistió en reconocer y registrar todas las falencias presentes en la situación actual de la empresa en relación a la seguridad de la información. Se buscó comprender el grado de cumplimiento de las medidas de seguridad vigentes y analizar las vulnerabilidades que ponen en peligro la integridad, confidencialidad y disponibilidad de la información.

Durante esta observación, se brindó una especial atención a los distintos parámetros claves que intervienen de manera directa y crítica con los activos de la empresa, como los controles de

acceso lógicos y físicos, los niveles de protección de datos, los incidentes de la seguridad de la información, políticas y procedimientos, continuidad del negocio y el manejo de la información.

4.6.2. Metodología utilizada en la observación

Para llevar cabo esta observación de las deficiencias de seguridad de la información en la empresa, se utilizó una combinación de varias técnicas. Entre estas se incluyen:

- **Observación directa:** Se realizó una visita a las instalaciones de la empresa para tener un panorama claro sobre el entorno físico, los sistemas informáticos y las prácticas se seguridad en vigencia.
- **Revisión documental:** Se revisaron las políticas, procesos y organigramas de seguridad existentes en la empresa.
- **Conversaciones directas con el personal:** Se habló directamente con el jefe de Área de Tecnologías y con la Líder Financiera sobre el estado actual de la empresa y la situación de las medidas de seguridad de la información en la empresa. Estas conversaciones permitieron obtener información adicional sobre las prácticas de seguridad y las vulnerabilidades desde el punto de vista de dos áreas cruciales en la empresa.

4.6.3. Identificación de los riesgos asociados a los parámetros de seguridad

Como resultado de la observación y de las técnicas empleadas para la investigación, se identificaron múltiples riesgos asociados a la seguridad de la información en la empresa. Algunos de estos riesgos se relacionan a:

- **Controles de acceso:** Existe una falta de controles adecuados de accesos lógicos y físicos que permiten a personas no autorizada acceder de manera fácil a las instalaciones de la empresa y a la información confidencial de la empresa.

- **Tamaño de la empresa:** Existe un crecimiento exponencial en el tamaño de la empresa en varios países lo que involucra un riesgo grave en las operaciones de la empresa.
- **Riesgo de pérdida de datos:** Existen deficiencias en los sistemas de respaldo internos y recuperación de datos en las áreas de la empresa en caso de un evento catastrófico o incidente.
- **Riesgo de fuga de información:** Existe una falta de políticas claras y medidas de protección para evitar la divulgación y filtración de datos sensibles de la empresa.
- **Manejo de usuarios y contraseñas:** Existe una falta de políticas que traten la importancia del manejo de los usuarios de la empresa mediante un Directorio Activo y un escaso conocimiento por parte de los usuarios sobre la importancia de una buena contraseña.
- **Falta de herramientas:** El uso de herramientas de seguridad tales como antivirus, software de Data Loss Prevention (DLPs), o Centro de Operaciones de Seguridad (SOC) es nulo dentro de la organización.
- **Fallas en la infraestructura:** Dentro de las instalaciones de la organización solo se maneja un tipo de router donde todas las personas, incluidos externos, clientes y proveedores, se conectan a un mismo servicio de red inalámbrica. Esto implica un riesgo grave ya que las personas pueden vulnerar las conexiones internas de la empresa y acceder a su información crítica.
- **Relación con proveedores:** Actualmente, no existen controles que estipulen la seguridad de la información con los proveedores y esto implica un riesgo con las operaciones de la empresa.

4.7. Parámetros de seguridad

En el contexto de esta investigación, se han establecido ciertos parámetros relacionados al campo de la seguridad informática como una línea base de apoyo para el desarrollo del análisis. Estos parámetros permiten conocer de manera detallada la situación actual de la empresa y describen de manera breve los lineamientos establecidos en la matriz de lineamientos de la norma ISO 27001.

4.7.1. Niveles de Seguridad

En la empresa Urban Lab Effect S.A.S, actualmente no se han establecido niveles de seguridad específicos ni se han asignado a los diferentes activos y categorías de información. La falta de establecimiento de niveles de seguridad puede generar un riesgo considerable para la protección de la información sensible y los activos de la organización. A continuación, se proporciona un análisis de esta situación:

- **Ausencia de niveles de seguridad**: La falta de niveles de seguridad implica que no se ha definido un marco o estructura para categorizar y proteger los activos de la empresa de acuerdo con su importancia y nivel de sensibilidad. Establecer niveles de seguridad permite asignar recursos y medidas de protección de manera adecuada, priorizando aquellos activos y categorías de información que requieren un mayor nivel de protección.
- **Determinación de niveles de seguridad:** Para establecer niveles de seguridad, es necesario realizar una evaluación exhaustiva de los activos y categorías de información de la empresa y todas sus áreas o unidades de apoyo. Esto implica identificar y clasificar los activos en función de su importancia y sensibilidad, teniendo en cuenta factores como el valor económico, el impacto operativo, la confidencialidad, la integridad y la disponibilidad de la información.

- **Asignación de niveles de seguridad:** Una vez establecidos los niveles de seguridad, se debe asignar a los diferentes activos y categorías de información. La asignación de niveles de seguridad se debe realizar considerando los resultados de la evaluación de activos y la importancia relativa de cada activo dentro de la empresa.

4.7.2. Protección de Datos

En la empresa Urban Lab Effect S.A.S, actualmente se carece de medidas y políticas adecuadas para la protección de datos. Esto representa un riesgo significativo para la seguridad de la información de la organización. A continuación, se presenta un análisis de la situación actual:

- **Copias de seguridad:** En la empresa, se realizan copias de seguridad de manera irregular en la nube. Sin embargo, no existe un control establecido sobre este proceso, lo que implica que no se siguen políticas y procedimientos definidos para garantizar la integridad y disponibilidad de los datos respaldados. Es crucial implementar un plan de copias de seguridad regular y documentado, que incluya frecuencia, ubicación de almacenamiento y métodos de recuperación.
- **Restricciones de acceso:** No se han establecido restricciones de acceso adecuadas a los datos en la empresa. Esto significa que cualquier empleado puede acceder a información sensible sin necesidad de autorización o justificación. Es necesario implementar políticas y controles de acceso basados en roles y privilegios, que garanticen que solo las personas autorizadas puedan acceder a los datos según su función y responsabilidad.
- **Cifrado de datos:** Actualmente, no se han implementado técnicas de cifrado de datos en la empresa. El cifrado de datos es una medida esencial para proteger la confidencialidad de la información, especialmente cuando se transmite o almacena en medios no seguros.

- **Ley Orgánica de Protección de Datos:** La empresa si cumple con la Ley Orgánica de Protección de Datos (LOPD). Sin embargo, es importante mencionar que el cumplimiento de esta ley no es suficiente para garantizar una protección integral de la información de la empresa y sus clientes.

4.7.3. Gestión de Incidentes de Seguridad de la Información

En la empresa Urban Lab Effect S.A.S, actualmente se carece de una gestión adecuada de los incidentes de seguridad de la información. La falta de procedimientos establecidos, asignación de responsabilidades y medidas correctivas representa un riesgo significativo para la protección de la información y la capacidad de respuesta de la organización frente a posibles incidentes. A continuación, se presenta un análisis de la situación actual:

- **Detección y notificación de incidentes**: En la empresa, cuando ocurre un incidente de seguridad de la información, el usuario simplemente lo comunica al jefe de TI para que lo resuelva. Esta falta de formalidad y procesos específicos para la detección y notificación dificulta la identificación temprana de los incidentes y la toma de acciones rápidas para su resolución.
- **Procedimientos establecidos**: Actualmente, no existe un plan de gestión de incidentes ni procedimientos establecidos para tratar la detección, notificación y seguimiento de los incidentes de seguridad de la información. Es fundamental establecer un marco de referencia que incluya pasos claros y procesos documentados para la gestión de incidentes, desde la identificación inicial hasta la resolución final para evitar problemas en el futuro.
- **Asignación de roles y responsabilidades**: En la empresa, no se han asignado responsabilidades específicas para la gestión de incidentes de seguridad de la información. Esto genera confusión y retrasos en la toma de decisiones y acciones adecuadas. Se recomienda definir roles y responsabilidades claras, designando a

personas responsables de la detección, notificación, investigación y resolución de los incidentes de seguridad de la información.

- **Comunicación interna y externa**: En la empresa no se han establecido procedimientos de comunicación interna y externa para los incidentes de seguridad de la información. La falta de una comunicación adecuada puede generar demoras en la respuesta, afectar la reputación de la empresa y la confianza de los clientes. Es vital establecer canales de comunicación claros y eficientes para notificar, informar y coordinar acciones relacionadas con los incidentes de seguridad de la información.
- **Medidas correctivas:** Actualmente, no existen medidas correctivas establecidas para los incidentes de seguridad de la información en la empresa. Es crucial definir acciones específicas que se deben tomar para solucionar los incidentes, mitigar su impacto y evitar su recurrencia.

4.7.4. Continuidad del Negocio

En la empresa Urban Lab Effect S.A.S, se han definido parcialmente planes para garantizar la continuidad del negocio en caso de interrupciones. Sin embargo, estos planes no están establecidos en políticas o documentos formales, lo que dificulta su difusión y conocimiento en el área de TI. Además, no todas las personas del equipo de TI están al tanto de estos planes debido a la falta de confianza dentro del área. A continuación, se presenta un análisis de la situación actual:

- **Planes de continuidad del negocio:** Aunque se han definido planes parcialmente, es necesario documentarlos en políticas y procedimientos formales. Esto permitirá que los planes sean accesibles para todos los miembros del equipo de TI y otros colaboradores relevantes. Estos planes deben abordar la recuperación de la información y la infraestructura necesaria para garantizar la continuidad del negocio en caso de interrupciones o desastres.

- **Pruebas periódicas:** Actualmente, las pruebas periódicas del sistema principal de la empresa (IDUKAY) son realizadas únicamente por el jefe de área. Esta falta de participación y conocimiento de los demás colaboradores puede afectar la efectividad de las pruebas y la capacidad de respuesta ante una interrupción real. Se recomienda involucrar a todos los miembros del equipo de TI en las pruebas periódicas para fomentar la colaboración y el conocimiento compartido.
- **Registro de pruebas y resultados:** En la empresa, los resultados de las pruebas periódicas son confidenciales y solo son documentados por el jefe de área. Esto limita el acceso a la información sobre el desempeño del sistema durante las pruebas y dificulta la identificación de mejoras o actualizaciones necesarias. Es importante y se recomienda establecer un registro centralizado de las pruebas realizadas y los resultados obtenidos, para que todos los miembros del equipo de TI puedan tener acceso a esta información y contribuir en la identificación de áreas de mejora.

4.7.5. Transferencia de Información Física y Digital

En la empresa Urban Lab Effect S.A.S., actualmente no se disponen de políticas ni procedimientos que traten la transferencia de la información física y digital y se han identificado una serie de deficiencias y carencias que afectan la seguridad de la transferencia de la información. A continuación, se presenta un análisis de la situación actual:

- **Falta de políticas y controles:** La empresa carece de una serie de políticas y controles establecidos para garantizar la correcta transferencia de la información física y digital. Esto significa que no se han establecido directrices claras sobre cómo deben manejarse los datos sensibles durante la transferencia, lo que puede resultar en riesgos de seguridad y violaciones de la confidencialidad.
- **Clasificación inadecuada de la información:** Uno de los grandes problemas identificados es que la empresa no ha clasificado adecuadamente su información por

niveles de importancia o confidencialidad. La falta de una clasificación adecuada dificulta la implementación de medidas de seguridad proporcionales a la sensibilidad de los datos y puede llevar a una transferencia insegura de información.

- **Ausencia de software:** La empresa no cuenta con un software de prevención de pérdida de datos (DLP), el cual es una herramienta vital para detectar y prevenir la fuga de la información confidencial. La falta de esta herramienta deja expuesta a la empresa a riesgos relacionados a la pérdida o robo de datos durante la transferencia de la información.
- **Carencia de antivirus:** La ausencia de un software antivirus en la empresa representa un riesgo significativo para la seguridad de la información durante la transferencia. Sin un antivirus actualizado, los sistemas pueden estar expuestos a ataques de malware y virus que podrían comprometer la integridad y confidencialidad de los datos durante el proceso de transferencia.

4.8. Resultados de la evaluación de la matriz

Se ha elaborado una matriz exhaustiva para el levantamiento de información de la empresa, donde se establecen y evalúan los siguientes puntos clave en concordancia con la normativa ISO 27001:

1. Políticas de seguridad de la información.
2. Organización de la seguridad de la información.
3. Seguridad relacionada con los recursos humanos.
4. Gestión de activos.
5. Control de acceso.
6. Criptografía.
7. Seguridad física y del entorno.
8. Seguridad de las operaciones.

9. Seguridad de las comunicaciones.
10. Adquisición, desarrollo y mantenimiento de sistemas de información.
11. Relación con proveedores.
12. Gestión de incidentes de seguridad de la información.
13. Aspectos de seguridad de la información de la continuidad del negocio.
14. Cumplimiento.

En esta matriz, se ha evaluado minuciosamente cada uno de estos parámetros en función del cumplimiento real de la empresa en comparación con los estándares aceptables. Además, se presenta la situación actual de la empresa en relación con el cumplimiento aceptable, identificando tanto las oportunidades de mejora como los puntos en los que se cumple con los estándares establecidos.

4.9. Explicación de los resultados

Según los resultados obtenidos de la evaluación de la empresa utilizando la matriz, se identificaron varias oportunidades de mejora en cuanto a la seguridad de la información. Estos resultados se presentan en las figuras a continuación para brindar evidencia visual de los hallazgos mencionados (ver Figuras 3-6).

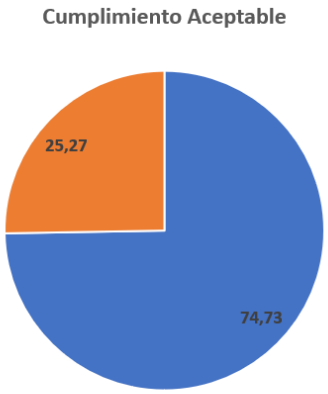


Figura 3 Gráfico de pastel donde se muestra la relación del estado real del cumplimiento (25,27%) con la oportunidad de mejora (74,73%) de la empresa.

Figura 4 Gráfico radial que representa el cumplimiento de la norma ISO 27001 en diferentes aspectos de seguridad de la información.

Estas figuras (ver Figuras 3-4) proporcionan una representación visual clara de los resultados obtenidos, lo que facilita la comprensión y permite identificar áreas específicas que requieren atención y mejoras en términos de seguridad de la información.

4.9.1. Explicación de resultados

Tras la evaluación de la empresa, se ha constatado que actualmente no se cumple en su totalidad con los lineamientos establecidos por la norma ISO 27001, así como tampoco con los requisitos básicos de la seguridad de la información. Se ha identificado una carencia significativa en cuanto a la documentación y procedimientos necesarios para garantizar un adecuado nivel de seguridad. En la tabla 5 se pueden evidenciar los resultados de la evaluación de las políticas

de seguridad de la información por cada aspecto junto con el cumplimiento aceptable, el cumplimiento real y el nivel esperado de cumplimiento.

Tabla 5 Resultados de la evaluación de las políticas de seguridad de la información alineado a la ISO 27001.

Dominio	Cumplimiento Aceptable	Cumplimiento Real	Nivel Esperado
1. Políticas de seguridad de la información	80	0	100
2. Organización de la seguridad de la información	80	18	100
3. Seguridad relativa a los recursos humanos	80	88	100
4. Gestión de activos	80	88	100
5. Control de acceso	80	6	100
6. Criptografía	80	0	100
7. Seguridad física y del entorno	80	38	100
8. Seguridad de las operaciones	80	20	100
9. Seguridad de las comunicaciones	80	18	100
10. Adquisición, desarrollo y mantenimiento de los sistemas	80	20	100
11. Relación con proveedores	80	17	100
12. Gestión de incidentes de seguridad de la información	80	6	100
13. Aspectos de seguridad de la información para la gestión	80	13	100
14. Cumplimiento	80	23	100

El cumplimiento real de la empresa en relación con la norma ISO 27001 se sitúa en un modesto 25,27%, lo cual indica la necesidad urgente de implementar mejoras y medidas correctivas. Existe una amplia oportunidad de mejora, que asciende al 74,73%, lo que implica un potencial significativo para elevar la seguridad de la información dentro de la organización. Como se muestra en la Figura 5, se puede observar el nivel de cumplimiento real en comparación con el cumplimiento aceptable de la empresa, según los estándares establecidos en la norma ISO 27001.

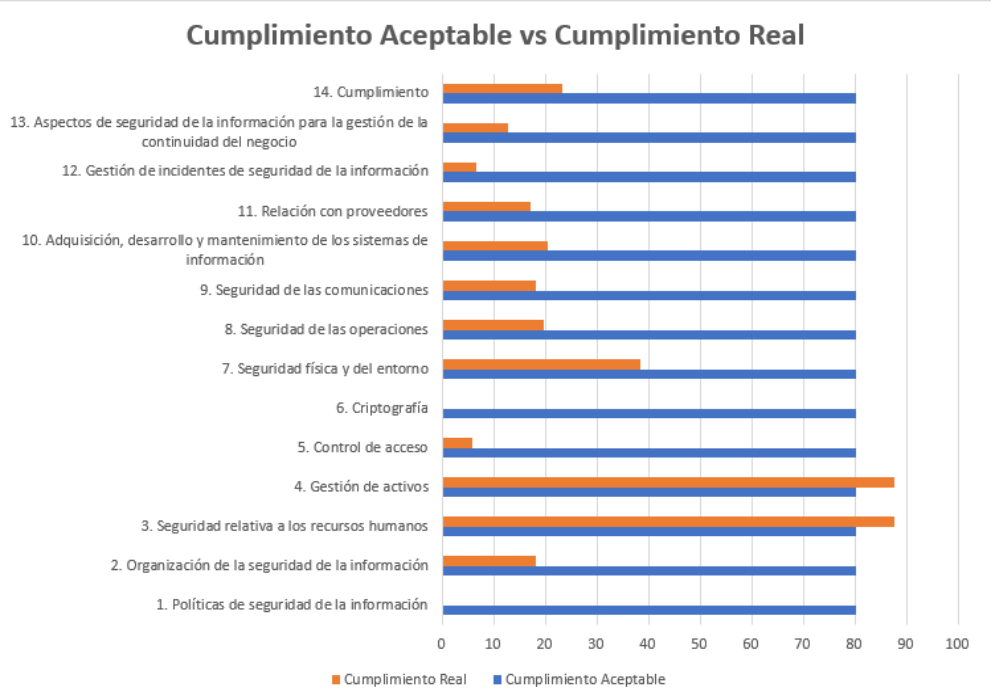


Figura 5 Cumplimiento Real vs Cumplimiento Aceptable de la empresa con relación a la norma ISO 27001.

Estos resultados revelan la importancia de enfocar los esfuerzos en fortalecer la implementación de los lineamientos de la norma ISO 27001, así como en establecer una sólida estructura de documentación y procedimientos. A través de la identificación y abordaje de estas áreas de oportunidad, la empresa podrá avanzar hacia una postura más sólida y confiable en materia de seguridad de la información, garantizando así la protección de los activos digitales y el cumplimiento de los estándares establecidos por la norma.

CAPÍTULO V: PROPUESTA DE IMPLEMENTACIÓN

5. Propuesta de plan de acción para la empresa

5.1. Objetivos de la propuesta

- Desarrollar y establecer un marco de seguridad de la información que proporcione los lineamientos básicos para para la correcta gestión de riesgos, protección de datos y la continuidad del negocio.
- Establecer políticas y medidas sobre la protección de datos, cifrado de información, control de accesos y monitoreo de brechas de seguridad.
- Desarrollar un plan de respuesta ante incidentes de seguridad de la información a mediano plazo para evitar potenciales incidentes en el futuro.

5.2. Alcance del plan de acción

Este plan de acción abarca de manera integral los principales aspectos relacionados con la seguridad de la información, siguiendo los parámetros establecidos por la norma ISO 27001. El plan establece las medidas necesarias para garantizar los niveles adecuados de seguridad, protección de datos, gestión de incidentes de seguridad de la información, así como la transferencia segura de la información en formato físiico y digital dentro de la empresa.

Además, el plan se ajusta a los términos y condiciones específicos de la empresa y debe seguir un cronograma establecido netamente por la empresa, teniendo en cuenta los recursos disponibles por parte de la organización.

5.3. Plan de acción en base a lineamientos de la norma ISO 27001

La Tabla 7 muestra de manera detallada los elementos clave de la propuesta del plan de acción que se recomienda a la empresa seguir, con el objetivo de garantizar una sólida seguridad de la información dentro de la organización. El plan de acción propuesto se centra en abordar los aspectos identificados en el análisis de seguridad de la información realizado en la empresa,

brindando una guía clara para mejorar y fortalecer la protección de los datos y recursos informáticos.

Tabla 6 Plan de Acción Base para la Empresa.

Lineamientos Clave	Propuesta de Plan de Acción / Hoja de Ruta
Niveles de Seguridad	• Establecer políticas de seguridad para la correcta gestión de la seguridad de la información en la empresa. • Realizar una política sobre la segregación de los roles y responsabilidades dentro de la empresa alineados a la seguridad de la información. • Realizar un levantamiento de activos de todos los procesos y áreas claves de la empresa y hacer el análisis de todos los riesgos relacionados alineados a la seguridad de la información.
Protección de Datos	• Implementar políticas que aborden aspectos como el acceso a los datos, manejo de contraseñas robustas, factores de doble autenticación y concientización en los trabajadores. • Realizar una evaluación de seguridad de la información a todos los proveedores para garantizar que cumplan con los estándares básicos de seguridad necesarios para proteger los datos de la empresa. • Implementar sistemas para la pérdida de datos como Microsoft Purview para evitar la fuga de información. (DLP) • Implementar el uso de controles criptográficos al igual que sus políticas y procedimientos. • Establecer una política de controles de accesos lógicos y físicos en la empresa. • Implementar licencias originales de los programas que se utilicen en la empresa. • Implementar el uso de una licencia empresarial de antivirus para toda la empresa.
Gestión de Incidentes de Seguridad de la Información	• Establecer políticas para la gestión de los incidentes de la seguridad de la información en la empresa. • Establecer un proceso formalizado para la correcta gestión de los incidentes de la seguridad de la información.

	• Establecer un mecanismo para la escalación de incidentes críticos. Como la inclusión de equipos de seguridad externos. • Establecer un plan de comunicación para informar y actualizar a todas las partes interesadas internas y externas sobre los incidentes de seguridad. • Brindar capacitación a los usuarios sobre la correcta gestión de los incidentes de la seguridad de la información. • Establecer un área especializada a los eventos relacionados a la seguridad de la información dentro de la empresa.
Transferencia de Información Física y Digital	• Establecer una política de clasificación de la información con la identificación de los niveles de confidencialidad en la empresa. • Implementar algoritmos de cifrado de datos seguros para la transferencia de la información. • Implementar acuerdos de confidencialidad con las empresas de mensajerías y proveedores. • Establecer un proceso de auditoría para verificar el cumplimiento de las políticas (a realizar). • Capacitar al personal sobre las buenas prácticas de la transferencia de la información.

5.4. Estimación de costos

Determinar una estimación precisa de los costos para cada elemento incluido en el plan de acción de la empresa resulta ser un proceso complejo debido a la influencia de diversos factores, como el tamaño de la organización, sus operaciones, infraestructura y presupuesto existente. Sin embargo, se destacan algunos factores clave a considerar para la implementación del plan de acción:

- Contratación de servicios de consultoría especializados.
- Adquisición e implementación de tecnología y herramientas específicas.
- Obtención de licencias necesarias.
- Contratación de personal especializado en Seguridad de la Información.

- Capacitación del personal de la empresa.
- Adquisición de nueva infraestructura, si es necesario.

En la ciudad de Quito existen diversas empresas especializadas en seguridad de la información, entre las que se incluyen LevelTech, Grupo Radical, GMS, entre otras. Se recomienda a la empresa solicitar cotizaciones personalizadas que se ajusten a su disponibilidad de recursos, plazos y otros factores relevantes.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- En la actualidad, la empresa Urban Lab Effect S.A.S muestra diversas vulnerabilidades y riesgos considerables en relación a la seguridad de la información. Este análisis ha evidenciado la ausencia de fundamentos básicos de seguridad de la información en la organización, lo cual la expone a múltiples brechas de seguridad. Es imperativo abordar todas estas vulnerabilidades para salvaguardar adecuadamente la integridad de la empresa.
- La empresa Urban Lab Effect S.A.S carece de una gestión adecuada de los incidentes de seguridad de la información y de planes formales de continuidad del negocio. La falta de procedimientos establecidos, asignación de responsabilidades y medidas correctivas representa un riesgo significativo para la protección de la información y la capacidad de respuesta de la organización frente a posibles incidentes o interrupciones. Es necesario implementar políticas, procedimientos y planes documentados, así como asignar roles y responsabilidades claras, para mejorar la gestión de incidentes y garantizar la continuidad del negocio.
- Al comparar las prácticas de seguridad de la información de la empresa con los estándares establecidos por las normas ISO 27001 y 27002, se evidencia un incumplimiento de los parámetros básicos requeridos para una gestión sólida de la seguridad de la información. Es fundamental que la empresa tome medidas correctivas urgentes para alinearse con estos estándares internacionales reconocidos. Esto implica establecer políticas y controles formales que aborden las deficiencias identificadas, como la transferencia segura de información, la clasificación adecuada de datos, la implementación de herramientas de prevención de pérdida de datos y antivirus, y el fortalecimiento de la conciencia y capacitación en seguridad dentro del equipo de TI. Cumplir con los estándares ISO 27001

y 27002 permitirá a la empresa mejorar su postura de seguridad de la información, proteger sus activos críticos y brindar confianza a sus clientes y socios comerciales.

Recomendaciones

- La alta gerencia de la organización, conformado por Gerencia General y Gerencia de Operaciones, debe reconocer la importancia de la seguridad de la información y proporcionar los recursos necesarios para poder llevar a cabo los planes de acción recomendados y subsanar todas las brechas identificadas. Esto implica una inversión moderada en materia de recursos como personal y tecnología. De esta manera, la inversión permitirá cumplir con los requisitos necesarios de las normas ISO y fortalecer su marca dentro del mercado.
- Se debe establecer un programa integral en materia de seguridad de la información donde se desarrollen e implementen todas las políticas y controles formales basados en los estándares ISO 27001 y 27002 para abordar las deficiencias identificadas en el análisis de seguridad. Además, incluir medidas como la transferencia segura de información, clasificación adecuada de datos, implementación de herramientas de prevención de pérdida de datos y antivirus, y fortalecimiento de la conciencia y capacitación en seguridad. Y asignar recursos y responsabilidades claras para garantizar la ejecución efectiva del programa y su integración en las operaciones diarias.
- Se debe mejorar la gestión de incidentes de seguridad y la continuidad del negocio mediante el desarrollo de un plan de continuidad del negocio donde se identifiquen los procesos críticos, recursos y medidas necesarias que garanticen la continuidad del negocio, además de brindar la capacitación adecuada a los empleados de la organización.

- Debido a que en la elaboración de este trabajo fue lanzada una nueva versión de la normativa ISO 27001:2022, se recomienda a la organización tomar como base los planes de acción recomendado y alinearlos a los reformados lineamientos de la norma.

BIBLIOGRFÍA

Almagro, C. A. (2011, Diciembre). *Universidad de Granada.* Obtenido de Departamento de Lenguajes y Sistemas Informáticos: https://lsi.ugr.es/curena/doce/lp/tr-11-12/lp-c01-impr.pdf

Anónimo. (2022, Julio 19). *ISO Tools*. Obtenido de ISO Tools: https://www.isotools.us/2019/06/11/iso-27002-la-importancia-de-las-buenas-practicas-en-los-sistemas-de-seguridad-de-la-informacion/

Eduardo Polo Ortega, F. J. (2015). *Servicios de red e Internet.* Madrid, España: RA-MA Editorial.

Grasa, J. M. (2017, 17 10). Acceso a Internet vía satélite. En J. Mora, *Guías de Tecnología fácil* (pág. 24). Madrid: Asociación española ingenieros de telecomunicación. Obtenido de http://www.coitaoc.org/files/estudios/tecnologia_facil_7aba8393.pdf

I. Fette, A. M. (2011, December). *Internet Engineering Task Force (IETF) .* Obtenido de https://www.hjp.at/doc/rfc/rfc6455.html

Instituto Nacional de Estadísticas y Censos. (2019). *www.ecuadorencifras.gob.ec.* Obtenido de https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2019/201912_Principales_resultados_Multiproposito_TIC.pdf

Kaspersky. (2018, Julio 30). *Support Kaspersky*. Obtenido de Support Kaspersky: https://support.kaspersky.com/KIS/2018/es-ES/82527.htm

Kaspersky. (s.f.). *Ransomware*. Obtenido de Ransomware: https://latam.kaspersky.com/resource-center/threats/ransomware

Kaspersky. (s.f.). *What is malware and how to protect against it. Kaspersky Resource Center.* . Obtenido de What is malware and how to protect against it. Kaspersky Resource Center. : https://latam.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it

Ley De Comercio Electrónico, Ley 67 (Congreso Nacional 05 17, 2002).

Ley Orgánica De Comunicación, 22 (Legislativo 06 25, 2013).

Onofa, M. (2022, Junio 30). *Dialogo Americas*. Obtenido de Dialogo Americas: https://dialogo-americas.com/es/articles/ataques-ciberneticos-amenazan-seguridad-en-ecuador/#.ZEqY0XbMK3C

Real Academia Española. (2021). REAL ACADEMIA ESPAÑOLA.

Sampieri, R. F. (2014). Definiciones de los enfoques cuantitativo y cualitativo, sus similitudes y diferencias. En C. F. Roberto Hernández Sampieri. RH Sampieri, Metodología de la Investivación.

Toro, R. (2021, Marzo 11). *PMG SSI - ISO 27001*. Obtenido de PMG SSI - ISO 27001: https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

Valencia, U. I. (2018, Abril 18). *Universidad VIU*. Obtenido de Universidad VIU: https://www.universidadviu.com/es/actualidad/nuestros-expertos/las-4-claves-de-la-seguridad-de-la-informacion

InfoCDMX. (s.f.). Protege tus datos personales: ¿Qué son los datos personales? Recuperado de https://www.infocdmx.org.mx/index.php/protege-tus-datos-personales/que-son-los-datos-personales.html

Finanzas Populares. (2021). Ley Orgánica de Protección de Datos Personales [PDF]. Recuperado de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Guaña-Moya, J., Chiluisa-Chiluisa, M. A., del Carmen Jaramillo-Flores, P., Naranjo-Villota, D., Mora-Zambrano, E. R., & Larrea-Torres, L. G. (2022, junio). Ataques de phishing y cómo prevenirlos Phishing attacks and how to prevent them. En 2022 17th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-6). IEEE.

Xataka. (s.f.). ¿Qué es un ataque DDoS y cómo puede afectarte? Recuperado de https://www.xataka.com/basics/que-es-un-ataque-ddos-y-como-puede-afectarte#:~:text=En%20esencia%2C%20un%20ataque%20DDoS,colapse%20y%20deje%20de%20funcionar.

ISO Tools. (s.f.). ISO 27001: norma internacional de seguridad de la información. Recuperado de https://www.iso27001standard.com/es/que-es-iso-27001

NQA. (s.f.). Guía de implantación de ISO 27001 [PDF]. Recuperado de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Sánchez, S. R. (2018). Implementación de políticas de seguridad de la información en una institución educativa [Tesis de maestría, Universidad Nacional Mayor de San Marcos]. Recuperado de https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/14862/Sanchez_sr.pdf?sequence=1&isAllowed=y

National Institute of Standards and Technology. (s.f.). Information Security Handbook: A Guide for Managers. Recuperado de https://www.nist.gov/publications/information-security-handbook-guide-managers?pub_id=50901

Fundamedios. (s.f.). Medio comunitario ecuatoriano sufrió ataque digital y quedó fuera del aire durante 5 horas. Recuperado de https://www.fundamedios.org.ec/alertas/medio-comunitario-ecuatoriano-sufrio-ataque-digital-y-quedo-fuera-del-aire-5-horas/

Proofpoint. (s.f.). DLP (Prevención de Pérdida de Datos). Recuperado de https://www.proofpoint.com/es/threat-reference/dlp

Primicias. (2023, junio 10). Ransomware: los pagos a cibercriminales millonarios. Primicias. Recuperado de https://www.primicias.ec/noticias/tecnologia/ransomware-pagos-cibercriminales-millonarios/#:~:text=El%20ransomware%20acecha%20al%20mundo,aseguran%20firmas%20como%20FortiGuard%20Labs

Global Suite Solutions. (s.f.). ¿Qué es la norma ISO 27001 y para qué sirve? Global Suite Solutions. Recuperado de https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/#:~:text=La%20norma%20ISO%2027001%20es,y%20disponibilidad%20de%20la%20informaci%C3%B3n

PMG SSI. (2016, Julio). ISO 27001:2013: los riesgos y las oportunidades. PMG SSI. Recuperado de https://www.pmg-ssi.com/2016/07/iso-27001-2013-los-riesgos-y-las-oportunidades/

BSI Group. (s.f.). ISO 27002: Controles de seguridad de la información. Recuperado de https://www.bsigroup.com/es-ES/iso-27002-controles-de-seguridad-de-la-informacion/

Norma ISO 27001. (s.f.). Recuperado de https://normaiso27001.es/

GLOSARIO DE TÉRMINOS

DLP: Software de Data Loss Prevention, es un software que previene la pérdida de datos sustanciales mediante políticas o directivas.

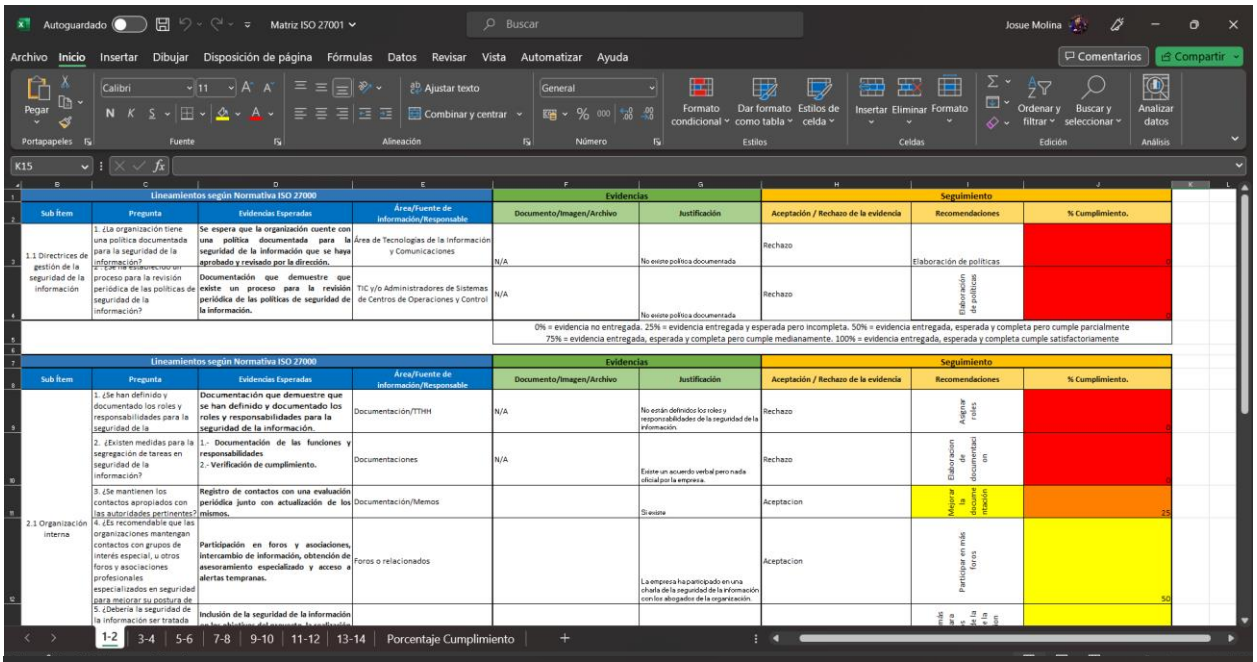
SOC: Es el equipo que está a cargo del centro de operaciones de seguridad de la información y que tiene como función principal monitorear, resguardar activos y proteger los sistemas y redes de una organización.

Antivirus: Es un programa informático diseñado principalmente para la detección, prevención y supresión de todo el software malicioso, como virus, malware y otras amenazas.

Firewall: Es un mecanismo de seguridad que regula el intercambio de información entre una red privada y una red externa. Su función consiste en examinar y decidir si permitir o bloquear el flujo de datos, estableciendo así una protección para la red para la organización.

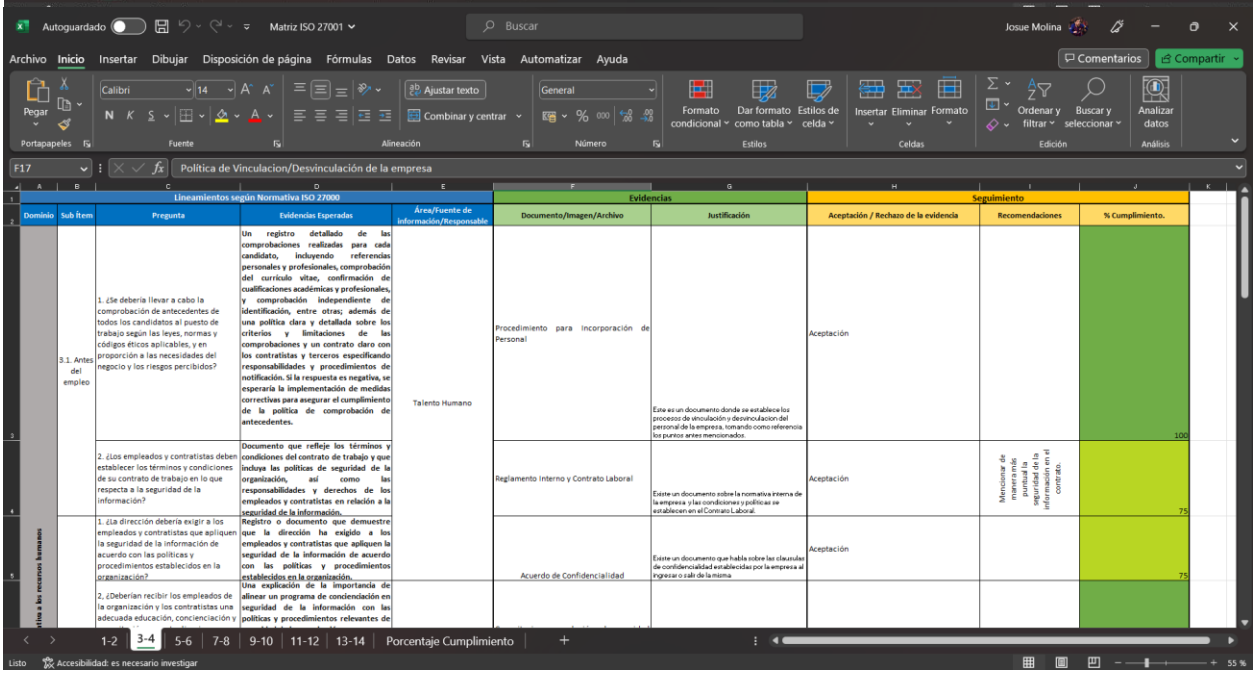
LOPD: Es la ley ecuatoriana encargada de regular la recopilación, el uso y la transferencia de todos los datos personales. Esta ley fue promulgada en mayo de 2021 por la Asamblea Nacional del Ecuador y su propósito radica en salvaguardar la confidencialidad y protección de la información personal de los individuos, asegurando así su privacidad y seguridad.

Anexo A: Matriz de Lineamientos según la Normativa ISO 27000.

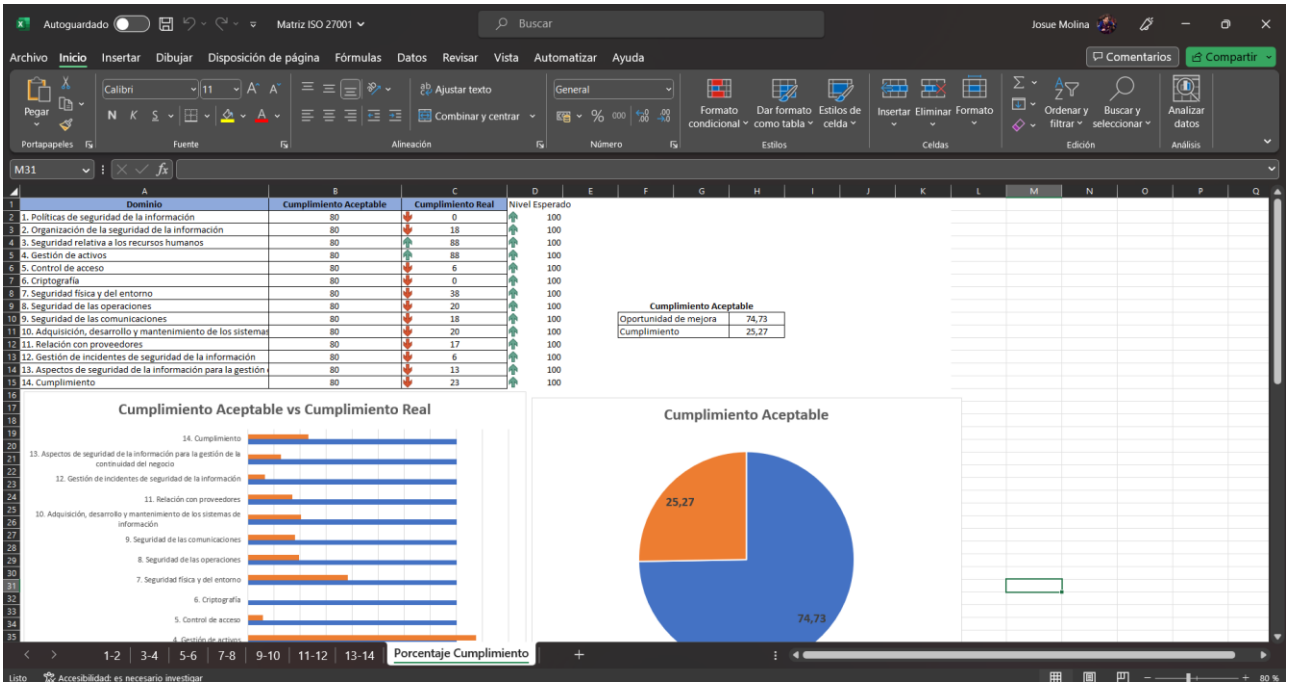


Lineamientos según Normativa ISO 27000				Evidencias		Seguimiento		
Sub Ítem	Pregunta	Evidencias Esperadas	Área/Fuente de información/Responsable	Documento/Imagen/Archivo	Justificación	Aceptación / Rechazo de la evidencia	Recomendaciones	% Cumplimiento.
1.1 Directrices de gestión de la seguridad de la información	1. ¿La organización tiene una política documentada para la seguridad de la información?	Se espera que la organización cuente con una política documentada para la seguridad de la información que se haya aprobado y revisado por la dirección.	Área de Tecnologías de la Información y Comunicaciones	N/A	No existe política documentada	Rechazo	Elaboración de políticas	
	2. ¿Se ha establecido un proceso para la revisión periódica de las políticas de seguridad de la información?	Documentación que demuestre que existe un proceso para la revisión periódica de las políticas de seguridad de la información.	TIC y/o Administradores de Sistemas de Centros de Operaciones y Control	N/A	No existe política documentada	Rechazo	Elaboración de políticas	
0% = evidencia no entregada. 25% = evidencia entregada y esperada pero incompleta. 50% = evidencia entregada, esperada y completa pero cumple parcialmente 75% = evidencia entregada, esperada y completa pero cumple medianamente. 100% = evidencia entregada, esperada y completa cumple satisfactoriamente								

Lineamientos según Normativa ISO 27000				Evidencias		Seguimiento		
Sub Ítem	Pregunta	Evidencias Esperadas	Área/Fuente de información/Responsable	Documento/Imagen/Archivo	Justificación	Aceptación / Rechazo de la evidencia	Recomendaciones	% Cumplimiento.
2.1 Organización interna	1. ¿Se han definido y documentado los roles y responsabilidades para la seguridad de la	Documentación que demuestre que se han definido y documentado los roles y responsabilidades para la seguridad de la información.	Documentación/TTHH	N/A	No están definidos los roles y responsabilidades de la seguridad de la información.	Rechazo	Asignar roles	
	2. ¿Existen medidas para la segregación de tareas en seguridad de la información?	1.- Documentación de las funciones y responsabilidades 2.- Verificación de cumplimiento.	Documentaciones	N/A	Existe un acuerdo verbal pero nada oficial por la empresa.	Rechazo	Elaboracion de documentación	
	3. ¿Se mantienen los contactos apropiados con las autoridades pertinentes?	Registro de contactos con una evaluación periódica junto con actualización de los mismos.	Documentación/Memos		Si existe	Aceptacion	Mejorar la documentación	25
	4. ¿Es recomendable que las organizaciones mantengan contactos con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad para mejorar su postura de	Participación en foros y asociaciones, intercambio de información, obtención de asesoramiento especializado y acceso a alertas tempranas.	Foros o relacionados		La empresa ha participado en una charla de la seguridad de la información con los abogados de la organización.	Aceptacion	Participar en más foros	50
	5. ¿Debería la seguridad de la información ser tratada	Inclusión de la seguridad de la información						



Lineamientos según Normativa ISO 27000					Evidencias		Seguimiento		
Dominio	Sub Ítem	Pregunta	Evidencias Esperadas	Área/Fuente de información/Responsable	Documento/Imagen/Archivo	Justificación	Aceptación / Rechazo de la evidencia	Recomendaciones	% Cumplimiento.
3. Antes de los recursos humanos	3.1. Antes del empleo	1. ¿Se debería llevar a cabo la comprobación de antecedentes de todos los candidatos al puesto de trabajo según las leyes, normas y códigos éticos aplicables, y en proporción a las necesidades del negocio y los riesgos percibidos?	Un registro detallado de las comprobaciones realizadas para cada candidato, incluyendo referencias personales y profesionales, comprobación del currículo vitae, confirmación de cualificaciones académicas y profesionales, y comprobación independiente de identificación, entre otras; además de una política clara y detallada sobre los criterios y limitaciones de las comprobaciones y un contrato claro con los contratistas y terceros especificando responsabilidades y procedimientos de notificación. Si la respuesta es negativa, se esperaría la implementación de medidas correctivas para asegurar el cumplimiento de la política de comprobación de antecedentes.	Talento Humano	Procedimiento para Incorporación de Personal	Este es un documento donde se establece los procesos de vinculación y desvinculacion del personal de la empresa, tomando como referencia los puntos antes mencionados.	Aceptación		100
		2. ¿Los empleados y contratistas deben establecer los términos y condiciones de su contrato de trabajo en lo que respecta a la seguridad de la información?	Documento que refleje los términos y condiciones del contrato de trabajo y que incluya las políticas de seguridad de la organización, así como las responsabilidades y derechos de los empleados y contratistas en relación a la seguridad de la información.		Reglamento Interno y Contrato Laboral	Existe un documento sobre la normativa interna de la empresa y las condiciones y políticas se establecen en el Contrato Laboral.	Aceptación	Mencionar de maneras más puntual la seguridad de la información en el contrato.	75
		1. ¿La dirección debería exigir a los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización?	Registro o documento que demuestre que la dirección ha exigido a los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.		Acuerdo de Confidencialidad	Existe un documento que habla sobre las cláusulas de confidencialidad establecidas por la empresa al ingresar o salir de la misma	Aceptación		75
		2. ¿Deberían recibir los empleados de la organización y los contratistas una adecuada educación, concienciación y	Una explicación de la importancia de alinear un programa de concienciación en seguridad de la información con las políticas y procedimientos relevantes de						



Enlace a OneDrive donde se encuentra la matriz: [Matriz ISO 27001.xlsx]

Anexo B: Procedimiento Ejemplo dentro de Idukay.

idukay

Procedimiento Gestión del Departamento de [redacted]

1. Objetivo: Definir los esquemas de trabaj[redacted]
[redacted]:

- [redacted] y la priorización de [redacted] equipo de desarrollo.
- [redacted]

2. Términos:

- **Requerimientos:**
  - **Funcional:** [redacted] funcionalidades existentes en los productos
  - **Bugs:** [redacted] sobre [redacted] funcionalidades actuales
  - **Estratégico:** [redacted] definidos por el equipo interno, normalmente la gerencia general o de operaciones que buscan la [redacted] necesidades estratégicas del negocio.
  - **Técnico:** [redacted] que garantizan el correcto funcionamiento de la plataforma
- **Fuente:** [redacted] o [redacted].
- **Canal:** [redacted]
- **Procesamiento** [redacted].

Anexo C: Acuerdo de Confidencialidad y Privacidad

Quito, 3 de mayo del 2023.

Acuerdo de Confidencialidad y Privacidad

Este Acuerdo de Confidencialidad y Privacidad se establece entre Urban Lab Effect S.A.S, con domicilio social en la Av. Diego de Almagro, Edificio. Almagro 240, en adelante Urban Lab Effect S.A.S, y Josué Iván Molina Gonzaga, con número de cédula 1726352113, estudiante de la Pontificia Universidad Católica del Ecuador.

CONFIDENCIALIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1.1 La Empresa se compromete a no proporcionar todos los requerimientos, políticas ni procedimientos relacionados con su seguridad de la información al estudiante, por cuestiones de privacidad y protección de datos.

1.2 El estudiante reconoce y acepta que toda la información, datos, documentos y cualquier otra forma de conocimiento o material proporcionado por la Empresa, incluyendo, pero no limitado a, información relacionada con su seguridad de la información, será considerada como información confidencial y propiedad exclusiva de la Empresa.

1.3 El estudiante se compromete a tratar toda la información confidencial proporcionada por la Empresa con el más alto grado de cuidado y confidencialidad, y a utilizarla únicamente para los fines establecidos en este Acuerdo.

EXCLUSIVIDAD

2.1 El Estudiante reconoce y acepta que el trabajo realizado en el marco de esta investigación tendrá exclusividad para la Empresa, y que no podrá compartir, divulgar, reproducir o utilizar de ninguna manera dichos resultados sin el consentimiento expreso y por escrito de la Empresa.

5.1 La Empresa se reserva el derecho de realizar cambios en la información proporcionada, así como de negar el acceso a cierta información en cualquier momento y por cualquier motivo, sin previo aviso al estudiante.

VIGENCIA Y TERMINACIÓN

6.1 Este Acuerdo entrará en vigor en la fecha de su firma por ambas partes y tendrá una duración de 90 días.

6.2 Cualquiera de las partes podrá dar por terminado este Acuerdo mediante notificación escrita a la otra parte, en caso de incumplimiento sustancial de cualquiera de las cláusulas establecidas en este Acuerdo.

LEY APLICABLE Y JURISDICCIÓN

7.1 Este Acuerdo se regirá e interpretará de acuerdo con las leyes de la República del Ecuador.

7.2 Cualquier disputa o controversia derivada de este Acuerdo será sometida a la jurisdicción exclusiva de los tribunales competentes del Distrito Metropolitano de Quito.

En prueba de conformidad, las partes firman el presente Acuerdo de Confidencialidad y Privacidad en dos ejemplares originales, uno para cada parte, en la fecha indicada a continuación.

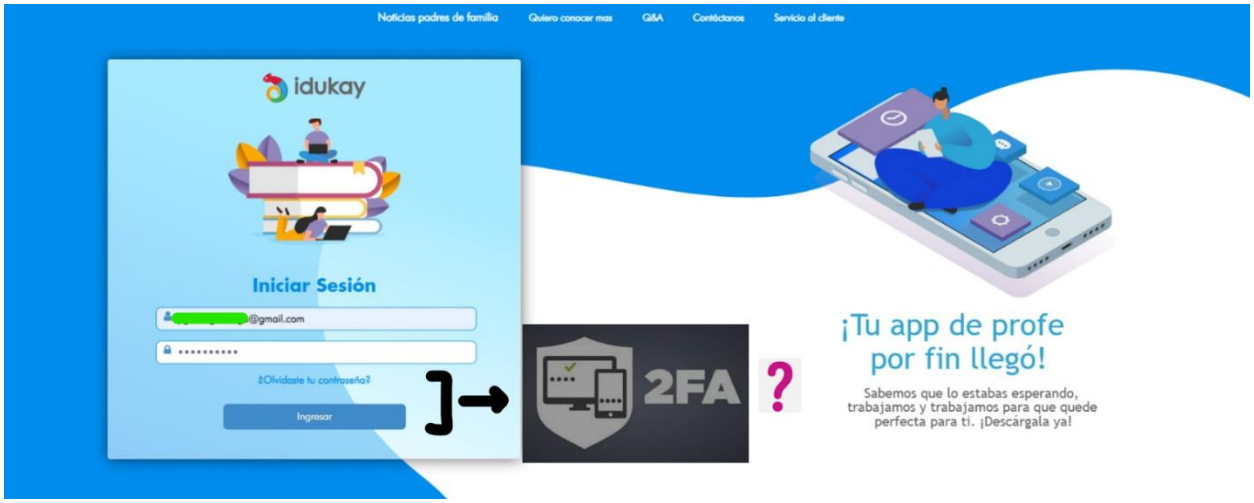
Representante de Urban Lab Effect S.A.S.

03/05/2023

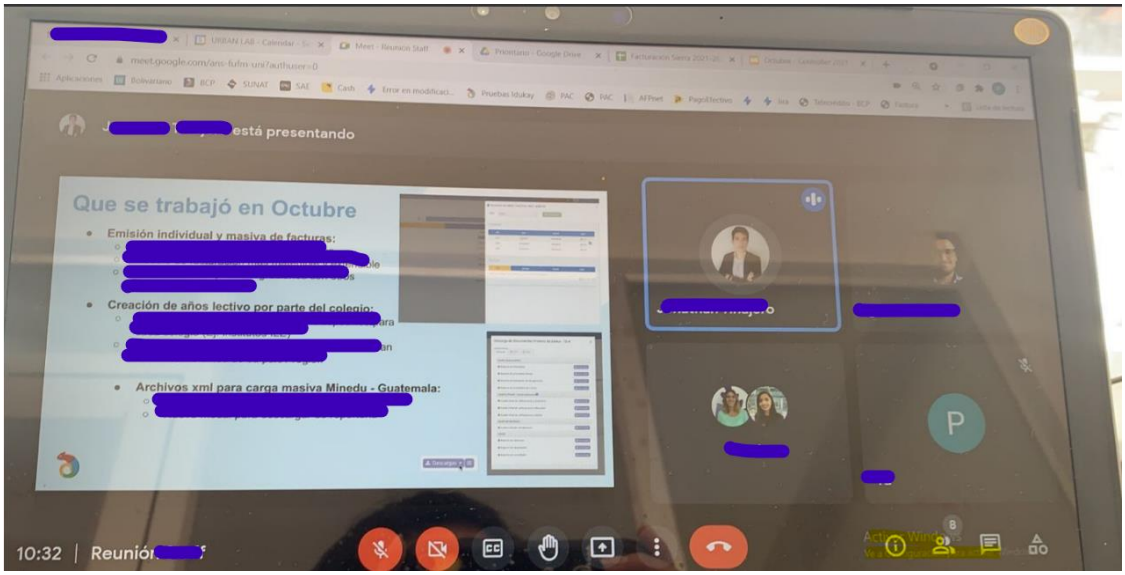
Josué Iván Molina Gonzaga

03/05/2023

Anexo D: Captura plataforma Idukay.



Anexo E: Fotografías


está presentando
Que se trabajó en Octubre
Emisión individual y masiva de facturas:
Creación de años lectivo por parte del colegio:
Archivos xml para carga masiva Minedu - Guatemala:
10:32 | Reunión