Evaluación de metodologías para sistemas de control de accesos en la Organización ECOLOGICAL INNOVA

Angie Gabriela Ávila García

Asesor

Christian Hernán Obando Ibarra

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Dedicatoria

Con gran gratitud y emoción, dedico este trabajo de grado titulado *"Evaluación de Metodologías para Sistemas de Control de Accesos en la Organización ECOLOGICAL INNOVA"* a todas las personas que han sido un apoyo fundamental en mi vida y en mi proceso académico.

A mis padres, por ser mi mayor ejemplo de esfuerzo, dedicación y amor incondicional. Gracias por enseñarme a luchar por mis sueños y estar siempre a mi lado en cada etapa de mi vida.

A mi familia, quienes con su apoyo y palabras de aliento hicieron que este sueño fuera posible. Su confianza en mí ha sido una fuente constante de motivación.

A mis docentes y mentores, especialmente a Dani León, por inspirarme a alcanzar la excelencia y por su valiosa orientación durante el desarrollo de este trabajo.

A mis amigos, que con su compañía y comprensión iluminaron los momentos difíciles y celebraron conmigo cada pequeño logro.

Y a todas aquellas personas que creen en el poder del conocimiento y en el impacto positivo que este puede tener en nuestra sociedad. Este trabajo es también para ustedes.

Agradecimientos

En primer lugar, agradezco a Dios por darme la fortaleza, perseverancia y salud necesarias para completar esta etapa de mi vida académica.

A mi tutor académico, Dani León, por su paciencia, asesoría constante y valiosos aportes durante todo el proceso. Su experiencia y orientación fueron clave para estructurar y enriquecer este trabajo.

A mis docentes y compañeros de la UNAD, por fomentar un ambiente de aprendizaje y discusión que contribuyó significativamente a mi formación.

A mi familia, que ha sido mi pilar incondicional. Gracias por su amor, apoyo y comprensión en los momentos más desafiantes de esta etapa. Su confianza en mí ha sido mi mayor motivación.

Finalmente, extiendo mi gratitud a todos los amigos y colaboradores que de una u otra manera contribuyeron al desarrollo de este trabajo. Sus palabras de aliento y consejos fueron esenciales para alcanzar esta meta.

A todos ustedes, gracias.

Resumen

Gracias a que las compañías están en crecimiento y desarrollo constante a fin de lograr una mayor competitividad en el mercado, teniendo en cuenta la globalización y la transformación digital, o mejor dicho con esta tercera revolución industrial que avanza de manera acelerada, surgen nuevos desafíos y con ellos nuevas amenazas a lo que necesariamente deben responder las compañías con estrategias que permitan apuntar a localizar y atender las diferentes amenazas, adoptando e implementando medidas sólidas para mitigarlas, lo que significa que se debe tener actualizadas las normas pertinentes que se ajusten a las necesidades de la compañía y que abarque todos los escenarios posibles de su infraestructura, como equipos físicos y los distintos sistemas de información.

Es importante que en la compañía se establezcan proyectos que permitan adecuar controles robustos que fortalezcan las medidas de seguridad para la información, con este fin se determina el enfoque en la estrategia que se debe aplicar para identificar los riesgos y como administrarlos de manera óptima y responsable, esto va encaminado con el marco de trabajo que se debe aplicar.

Dado lo anterior en la compañía ECOLOGICAL INNOVA, se identificó el estado actual de la compañía, y la estrategia de seguridad existente, analizando cuales son los puntos en los cuales se determinan ausencias y poder implementar las iniciativas en el plan director. (Gomez & Perez, 2018)

Palabras clave: Seguridad, Amenazas, Mitigación, Estrategias, Competitividad.

Abstract

Thanks to the constant growth and development of companies aiming to achieve greater competitiveness in the market, considering globalization and digital transformation, or better said, this third industrial revolution that is advancing at an accelerated pace, new challenges arise, and with them, new threats to which companies must necessarily respond with strategies aimed at identifying and addressing these various threats. This involves adopting and implementing solid measures to mitigate them, meaning that relevant regulations must be updated to suit the company's needs and cover all possible scenarios of its infrastructure, such as physical equipment and different information systems.

It is important for the company to establish projects that allow for the adaptation of robust controls that strengthen information security measures. To this end, the focus is determined on the strategy that should be applied to identify risks and manage them optimally and responsibly, aligned with the framework to be applied.

Given the above in the company ECOLOGICAL INNOVA, we identified the current state of the company, and the existing security strategy, analyzing which are the points in which absences are determined and to implement the initiatives in the master plan. (Gomez & Perez, 2018)

Keywords: Security, Threats, Mitigation, Strategies, Competitiveness.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Tabla de Apéndices

Introducción

La ciberseguridad es una realidad para las personas y las organizaciones del mundo contemporáneo. Es un concepto que, si bien parece complejo, a veces es más simple y necesario de entender. En un escenario digital la seguridad virtual es tan importante como la seguridad real en nuestras comunas o barrios. La definición del término ciberseguridad "Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entornó"

Las Vulnerabilidades de los sistemas informáticos se han convertido en una necesidad para cada aspecto de la vida diaria por lo que cantidades inmensas de información son generadas cada segundo, tanto por usuarios como empresas; por lo que no es extraño que usuarios malintencionados intenten acceder a estos sistemas para extraer esta información y conseguir un lucro económico.

Muchas son las herramientas creadas para la defensa de un sistema informático a través de una perspectiva ofensiva y defensiva. Por lo que la implementación de sistemas especializados para mitigar las amenazas informáticas está a la orden del día; no obstante, el eslabón más débil de la cadena de seguridad es y seguirá siendo el ser humano.

Esta monografía tiene como propósito evidenciar el estudio realizado en la empresa ECOLOGICAL INNOVA en la cual se identificaron diversas vulnerabilidades en la gestión de la información y seguridad informática, también se plantea la implementación de sistemas de acceso mediante biometría y reconocimiento facial para así no tener más vulnerabilidades y ser reconocida a nivel nacional por sus productos e innovación tecnológica.

Planteamiento del Problema

Las empresas en general se ven enfrentadas a muchas amenazas y vulnerabilidades en sus operaciones, son muy pocas las compañías que poseen un sistemas completo y robusto de controles de acceso y seguridad de la información, sin embargo, muchos de los principales autores de esta problemática se deben no solo a la falta de controles y políticas de seguridad en lugar de los procederes de colaboradores con acceso directo y permisos dentro de las mismas empresas. Es importante conocer todas aquellas amenazas y vulnerabilidades que nos expone la norma ISO 27001. (Tabla 1)

La empresa ECOLOGICAL INNOVA, a lo largo de su trayectoria ha presentado varias situaciones de perdida, robo de información y vulneración de acceso. Se obtuvo del departamento de tecnología la siguiente información, teniendo en cuenta que los datos específicos y/o puntuales no son divulgados, ni soporte de lo sucedido, solo generalidades.

Tabla 1

Información Innova

Año	Problema	Implicado	Descripción de lo sucedido	Solución
2017	Extracción base de datos clientes	Asesor comercial	Se identifica gracias a un tercero externo que un asesor comercial vendió la base de datos de clientes activos a la competencia, se analiza el computador del empleado y efectivamente se logra hallar los archivos que tenia de todos los clientes que la compañía tenía.	Cancelación del contrato a empleado, demanda por robo de información de la compañía, comunicado general a los clientes, con recomendaciones ante posibles fraudes.
2018	Ingreso y robo por tercero de equipo de computo	Tercero ayudado por personal de vigilancia	Se infiltra un tercero, con identificación falsa, carnet de la compañía falso hasta las oficinas, como son bahías, en un momento de ausencia del personal logra hurtar 2 computadores.	Gracias a registro de cámaras y declaraciones de vigilantes se logra

Nota. Elaboración Propia.

En el ámbito organizacional, la implementación de sistemas de control de acceso es fundamental para proteger los activos de información y mitigar riesgos asociados a amenazas internas y externas. Las organizaciones enfrentan desafíos significativos cuando carecen de políticas de seguridad robustas, y estos riesgos se agravan debido al factor humano, especialmente en relación con el manejo de accesos y permisos. En este contexto, surge la necesidad de diseñar estrategias efectivas que combinen tecnología, normativas claras y capacitación del personal. (ICONTEC, Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de Seguridad de la Información, 2022)

Con base en lo anterior se plantea la siguiente pregunta:

¿De qué manera ECOLOGICAL INNOVA puede establecer un sistema de controles de acceso, para reducir las amenazas y vulnerabilidades derivadas tanto de la ausencia de políticas de seguridad como de las acciones asociadas al factor humano con acceso y permisos dentro de la organización?

Justificación

La presente monografía se enfocará en el estudio y análisis de las políticas y estrategias de control para la seguridad de la información, acceso y activos de la empresa ECOLOGICAL INNOVA, buscando identificar como están implementadas, su uso y aplicación de cara a empleados y terceros como agentes externos. El estudio tiene como propósito realizar la investigación y análisis del estado de una empresa en Colombia de tal manera que se pueda aplicar un plan director de seguridad (PDS), para este caso se escogerá la compañía ECOLOGICAL INNOVA, una multinacional que se dedica a la comercialización de materias primas (químicos), para todas las industrias y a la cual se le realizará una revisión y estudio para identificar su estado teniendo en cuenta los ítems: Alcance del plan director de seguridad (PDS), Objetivos del alcance del plan director de seguridad (PDS), Análisis y valoración de riesgos, Declaración de aplicabilidad, GAP 27001 y Auditorías de Seguridad de la información, basado en estos conceptos, se indagará sobre la estrategia que maneja la compañía identificando así los objetivos estratégicos que maneja con el fin de poder aplicar la gestión de seguridad informática en sus procesos y gestiones de los sistemas de información. (Arboleda, 2021)

Se busca identificar en qué situación la compañía requiere fortalecer la gestión de seguridad, o si por el contrario no existe gestión alguna, iniciar el proceso para adecuar la implementación, bien sea en los enfoques de actualización y/o aseguramiento de la tecnología, gestión de procesos o ajuste y aplicación de gestión normativa nacional o internacional. Este proceso de implementación se realizará mediante la presentación del plan estructurado por el equipo investigador y propuesto mediante 10 proyectos aplicables a la compañía ECOLOGICAL INNOVA, mediante un informe ejecutivo firmado por líderes de equipo. (Correa, 2017)

Objetivos

Objetivo General

Evaluar las metodologías de seguridad y control para la organización ECOLOGICAL INNOVA, con el fin de identificar y reducir amenazas y vulnerabilidades derivadas tanto de la ausencia de políticas de seguridad como de las acciones asociadas al factor humano con acceso y permisos dentro de la organización.

Objetivos Específicos

Comparar metodologías de seguridad y control para el uso adecuado de las políticas de seguridad para ECOLOGICAL INNOVA, a través de una revisión bibliográfica, y determinar las mejores prácticas identificadas dentro de la organización.

Identificar las amenazas potenciales y las soluciones dentro del marco de la ISO 27001 para mitigar los riesgos y vulnerabilidades identificados en la organización.

Desarrollar un plan de acción basado en la norma ISO 27001 para implementar medidas de seguridad efectivas que mitiguen los riesgos y vulnerabilidades identificados en la organización.

Marco Referencial

Antecedentes

"En definitiva, las amenazas son externas a los activos de información, y las vulnerabilidades suelen ser atributos o aspectos del activo que la amenaza puede explotar. Si bien las amenazas tienden a ser externas a los activos, no provienen necesariamente de fuera de la organización. De hecho, la mayoría de los incidentes de seguridad de la información de hoy se originan dentro del perímetro de la organización" (Escuela Europea de Excelencia, 2024)

Tabla 2

Amenazas - Vulnerabilidades

Amenazas	Vulnerabilidades
Acceso de personas no autorizadas a la red de información	Usuarios con interfaces complicadas
Ataques y amenazas con bombas	Contraseñas predeterminadas sin no titilación ni autorización
Relaciones contractuales vulneradas	Medios de almacenamiento de datos eliminados
Infracciones de tipo legal	Daños a los equipos por cambios de voltaje
Desvió de información confidencial	Equipos expuestos a contaminación y humedad
Identidad de un usuario oculta	Mal cableado
Daños causados por terceros	Capacidad del sistema inadecuado
Daños por pruebas de penetración	Cambios inadecuados de sistemas
Registros destruidos	Información mal clasificada
Desastres por causas humanas	Acceso físico sin control
Desastre natural	Inadecuado mantenimiento
Revelar información a terceros	Gestión de la red inadecuada
Divulgar contraseñas	Irregular respaldo de información
Fraude y malversación	Error e inadecuado de protección de contraseñas
Errores por mantenimientos preventivos	Protección física inapropiada
Fallo en enlaces de comunicación	Error en cambio de equipos inadecuados
Registros falsificados	Falta de conciencia sobre seguridad en colaboradores
Espionaje industrial	Segregación inadecuada de funciones
Desaparición de información	Segregación errónea en instalaciones operativas
Procesos de negocios interrumpidos	Deficiencia en la supervisión de empleados y terceros
	Malas especificaciones e incompletas en el desarrollo de software
Perdida eléctrica	Pruebas de software insuficientes
Perdida de servicio de apoyo	Ausencia de política de acceso remoto

Amenazas	Vulnerabilidades
Equipos obsoletos o con daños	Ausencia de política de escritorio limpio y pantalla clara
Códigos maliciosos	No control de datos de entra y salida
Mal usos de los sistemas de información	Documentación interna incompleta
Mal manejo de las herramientas de auditoria	Falencia en la implementación de auditoría interna
Contaminación	Criptografía con falta de políticas
Software defectuoso con errores	Procedimientos incompletos para eliminar derechos de acceso a la terminación de empleo
Huelgas o paros	Equipos móviles desprotegidos
Terrorismo	Faltantes de redundancia y copias respaldadas
Hurtos por vandalismo	Falta de sistemas de identificación y autenticación
Cambio de datos en un sistema de información de manera involuntaria	Datos sin procesar y sin validar
Cambios de registros sin autorización	Riesgo de inundaciones en lugares donde estén los equipos
Instalaciones de software no autorizados	Datos de prueba errados
Acceso físico sin autorización	Copias de datos sin control
Material copyright sin autorización	Descargas de internet no controladas
Usos de software no autorizados	Sistemas de información incontrolados
Error de usuario	Software sin documentación legal
	Recurso humano desmotivado
	Redes públicas y conexiones de red desprotegidas
	Derechos de usuario sin revisión

Nota. Elaboración Propia

La súper Intendencia de Industria y Comercio en su rol de auditoría de control nacional y protección de datos, realizo el segundo estudio que abarco desde el año 2019 y 2020 sobre las medidas de seguridad implementadas por 33.596 de empresas privadas y entidades públicas, estos fueron los resultados. (Figura 1) (La Superintendencia de Industria y Comercio, 2023)

Figura1

Industria y Comercio

	2019	2020
Número de organizaciones evaluadas	32.763	33.596
No tienen una política de protección para acceso remoto a la información personal	88%	72.7%
No cuenta con mecanismos de monitoreo de consulta de las bases de datos	84%	69.3%
No ha implementado un procedimiento de auditoria de los sistemas de información	83%	71.3%
No tiene implementado un sistema de gestión de seguridad o un programa integral de gestión de datos	82%	67.5%
No ha implementado medidas especiales para proteger datos sensibles	79%	61.3%
No ha implementado una política de seguridad para el intercambio físico o electrónico de datos	76%	66.1%
No tiene política de auditoria de seguridad de la información	72%	63.6%
No tiene controles de seguridad en la tercerización de servicios para el tratamiento de datos	71%	61%
No implementa medidas apropiadas y efectivas de seguridad	66%	50.7%
No cuenta con herramientas de gestión de datos	63%	49.9%
No tiene políticas y procedimientos de gestión de incidentes de seguridad	62%	52.6%
Promedio de incumplimiento respecto de los ítems evaluados	**75.09%**	**62.36%**

Nota. Tomada de Industria y Comercio Súper Intendencia (2020).

El control de acceso físico ha sido un componente fundamental en las estrategias de seguridad de muchas organizaciones durante varias décadas. Al igual que ha sucedido con las demás tecnologías, el control de acceso ha evolucionado en el curso de los años y en este momento las soluciones ofrecen más seguridad y comodidad que nunca.

Con el fin de ilustrar mejor la importancia que tiene actualizar a la última tecnología de control de acceso, el presente documento analiza la evolución de las tarjetas y credenciales desde los años ochenta hasta la actualidad. Así mismo se examinan las tecnologías disponibles en la

actualidad y el futuro prometedor del control de acceso, además de aclarar por qué el uso de tecnología de control de acceso obsoleta puede poner en riesgo las organizaciones.

Marco Conceptual

La biometría es una herramienta clave que permite identificar a las personas mediante métodos como el reconocimiento manual, facial o el uso de tarjetas. Su implementación es común en empresas, colegios y otras organizaciones para gestionar el acceso de forma controlada (Kaspersky, 2024)

Por otro lado, la seguridad de la información abarca todas las medidas preventivas y reactivas que las organizaciones y los sistemas tecnológicos adoptan para proteger sus datos. Estas medidas están diseñadas para garantizar la confidencialidad, integridad y disponibilidad de la información, minimizando así los riesgos relacionados con su gestión (Esginnova Group, 2024)

En un ámbito más específico, la ciberseguridad se centra en la protección de redes, dispositivos móviles, sistemas electrónicos y datos frente a posibles ataques malintencionados. Es una disciplina esencial en la era digital actual (Kaspersky, 2024)

Los datos, por su parte, son información valiosa que puede referirse a empresas, individuos, organizaciones o entidades. Se utilizan principalmente en contextos estadísticos e informáticos, siendo un recurso fundamental en la toma de decisiones (IBM, 2024)

El concepto de riesgo se asocia a la posibilidad de que ocurra un daño o perjuicio, así como a las consecuencias derivadas de dicho evento. Este puede afectar tanto a individuos como a grupos y surge de acciones o eventos concretos (Concepto, 2024)

El acceso, en el contexto de la seguridad de la información, implica procesos de identificación, autenticación y autorización que permiten a los usuarios interactuar con sistemas, recursos o áreas específicas de manera controlada y segura (Senado de la republica, 2023)

La gestión de riesgos incluye procesos como la estimación e identificación de estos. La estimación del riesgo evalúa la probabilidad y las posibles consecuencias de un evento adverso, mientras que la identificación de riesgos busca localizar y caracterizar todos los elementos asociados a potenciales amenazas (Corporación autonoma regional del valle del cauca, 2020)

Finalmente, el impacto de un riesgo se traduce en un cambio negativo que puede afectar el logro de los objetivos organizacionales, comprometiendo el desarrollo y éxito de los negocios (ANI, 2019)

Marco Teórico

El control de acceso es sumamente importante para que todos los usuarios tengan el acceso correspondiente a datos y recursos de sistema. Todas las empresas tienen algunos desafíos previos a implementar todo este sistema ya que es un proceso de transición. Algunos de ellos son:

Comprensión de los Requisitos de Seguridad

Conocer cuáles van a ser los requisitos de seguridad del sistema, es el primer paso para diseñar un árbol de control de acceso. Esto nos ayuda a establecer los permisos adecuados. En este campo, se incluye la identificación de los datos sensibles, determinar quiénes van a tener acceso, y establecer diferentes procedimientos para manejar y proteger toda la información.

Cumplir los Estándares Necesarios

Hoy en día tenemos leyes que hablan directamente sobre el tratamiento de los datos, y de cómo estos se van a utilizar. Estando tan regulado, se obliga a las empresas a tomar las medidas

de seguridad oportunas para que se puedan cumplir estrictamente todos los requisitos de seguridad.

Gestión De Accesos Remotos

La creciente tendencia al teletrabajo, ha ocasionado que sea necesario realizar una gestión centralizada en este aspecto. Por lo cual siempre es importante revisar de forma periódica el acceso a todos los sistemas y datos que pueden ser sensibles.

Monitorización Y Auditorías

Mantener los sistemas bajo monitorización y realizar auditorías periódicas, nos ayuda a estar prevenidos ante casi cualquier problema que se pueda legar a presentar. Prevenir todos los problemas es la mejor forma de evitarlos y así tener en cuenta los controles de acceso de la empresa e ingresos de turnos.

Casos de Éxito en la Implementación de Sistemas de Control de Acceso

Complejo de Osong, es un lugar especializado para la salud donde organizaciones públicas como la Secretaría de Seguridad de Alimento y Medicamento, el Instituto Nacional de Salud, el Centro de Control y Prevención de Enfermedades lideran estudios de enfermedades y fomentan el desarrollo de la industria de la salud. (Tecno Seguros, 2022)

Industria. Complejo industrial.

Implementación. Sistema de control de acceso de Suprema, que incluye lectores de tarjetas, terminales de reconocimiento facial y controladores centrales.

Resultado. Mejora significativa en la seguridad y eficiencia operativa del complejo.

Empresa de Tecnología. Hoy en día, la protección de datos e instalaciones es una prioridad para empresas de cualquier tamaño. Los sistemas de control de acceso se han vuelto esenciales para resguardar los activos y optimizar la eficiencia operativa. En este artículo,

analizaremos cómo estos sistemas pueden mejorar la seguridad en las organizaciones, sus beneficios, tipos y factores clave a considerar al implementarlos. (Revista Seguridad 360, 2024)

Industria. Tecnología.

Implementación. Sistema de control de acceso basado en biometría.

Resultado. Reducción del 50% en los incidentes de seguridad en sus instalaciones.

Edificio Corporativo ABC. El edificio corporativo ABC implementó un sistema biométrico de control de acceso, lo cual incrementó la seguridad al prescindir de tarjetas físicas y simplificó el registro de entradas y salidas del personal. Esto les permitió ejercer un control más preciso sobre los accesos y optimizar la respuesta frente a posibles incidentes. (Revista Seguridad 360, 2024)

Industria. Corporativa.

Implementación. Sistema de control de acceso biométrico.

Resultado. Eliminación del uso de tarjetas físicas y facilitación del registro de entradas y salidas de los empleados.

Instituciones Financieras. La seguridad es una prioridad fundamental. Los sistemas de videovigilancia no solo brindan protección contra robos y actos de vandalismo, también ofrecen beneficios adicionales que pueden optimizar la eficiencia operativa y reforzar la seguridad de los empleados. (Revista Seguridad 360, 2024)

Industria. Financiera.

Implementación. Sistemas de acceso multifactor.

Resultado. Refuerzo significativo en la seguridad de sus operaciones.

Marco Legal

La compañía implementa los marcos normativos ajustados a y basados a la normatividad internacional como NIST y Sans CIS, para garantizar la protección de la información a cargo de las diferentes áreas y funcionarios de la compañía brindando las herramientas para el control de modificación accidental o divulgación no autorizada.

Norma Técnica Colombiana NTC- ISO/IEC colombiana 27001:2013. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información, las cuales están definidas y direccionadas al control, seguimiento y monitoreo los diferentes accesos que se tienen en las empresas de cara a la información contempladas dentro de las políticas definidas por las organizaciones limitando dicho acceso a la información e instalaciones de procesamiento de información.

Marco Contextual

ECOLOGICAL INNOVA es una compañía colombiana que nació en el año de 1.999, con el objetivo de distribuir materias primas para el sector farmacéutico. Hoy en día ECOLOGICAL INNOVA es una compañía líder en la distribución de materias primas en diversos mercados y atiende a un grupo importante de industrias.

El control de acceso en compañía ECOLOGICAL INNOVA se puede implantar a través de diferentes métodos. Estos mecanismos se eligen en función de las necesidades particulares de la compañía del nivel de seguridad deseado.

Por Teclado

Se basa en dispositivos que cuentan con un teclado en el que el usuario debe introducir un código numérico. Este código identifica al trabajador y desbloquea el acceso a un área determinada.

Por Huella Dactilar

El reconocimiento de la huella dactilar es un control de acceso biométrico que se basa en el hecho de que no existen dos huellas dactilares iguales. Es uno de los sistemas más habituales y se puede usar tanto para acceder a instalaciones.

Reconocimiento Facial

El reconocimiento facial o el ocular son otros sistemas de identificación biométricos. Se basan en un software que analiza los rasgos de la cara de una persona y comprueba sí coinciden con los de alguna entrada de su base de datos.

Objetivo 1

Comparar metodologías de seguridad y control para el uso adecuado de las políticas de seguridad para ECOLOGICAL INNOVA, a través de una revisión bibliográfica, y determinar las mejores prácticas identificadas dentro de la organización.

Definir Las Políticas De Seguridad Solida

Para definir las políticas de seguridad de la empresa se debe analizar el grado de cumplimiento de las prácticas de la materia de prevención de riesgo de la empresa, también validar los puntos fuertes y débiles con los que cuenta la empresa la construcción de las políticas se según las necesidades que se requieran.

Protección de Recursos

El esquema de protección de recursos garantiza que solo los usuarios autorizados podrán acceder a los objetos del sistema. La capacidad de asegurar todo tipo de recursos del sistema es una de las ventajas del Sistema. Primero se debe definir con precisión las distintas categorías de usuarios que pueden acceder al sistema. Asimismo, al momento de elaborar la política de seguridad, se debe definir qué tipo de autorización de acceso desea otorgar a estos grupos de usuarios y teniendo en cuenta de manera detallada y uno a uno el perfil y datos personales dentro de la organización.

Autenticación

Es la seguridad o la verificación de que el recurso (persona o máquina de Biometría) situado en el otro extremo de la sesión es realmente el que dice ser. Una autenticación convincente defiende el sistema contra riesgos de seguridad como las imitaciones, en las que el remitente o el destinatario utiliza una identidad falsa para acceder al sistema. Tradicionalmente, los sistemas han utilizado contraseñas y nombres de usuario para la autenticación; los

certificados digitales pueden ofrecer un método más seguro de autenticación, a la vez que proporcionan otras ventajas de seguridad. Cuando enlaza su sistema con una red pública como Internet, la autenticación de usuario toma nuevas dimensiones. Una diferencia importante entre Internet y una intranet es la capacidad de confiar en la identidad del usuario que inicia la sesión. Por lo tanto, se debe considerar seriamente la posibilidad de utilizar unos métodos más potentes de autenticación que los que proporcionan los procedimientos tradicionales de conexión mediante nombre de usuario y contraseña. Los usuarios autenticados podrían tener distintos tipos de permisos, según su nivel de autorización esto depende del área o departamento en el que se encuentre el trabajador y también nos influye el tipo de cargo en las organizaciones así la persona de soporte especializado entregara el usuario y los diferentes permisos y claves correspondientes a la plataforma, por otro lado, en el tema de accesibilidad ya sería reconocimiento facial y biometría dactilar.

Autorización

Es la seguridad de que la persona o el sistema situado en el otro extremo de la sesión tiene permiso para llevar a cabo la petición. La autorización es el proceso de determinar quién o qué puede acceder a los recursos del sistema o ejecutar determinadas actividades en un sistema. Normalmente, la autorización se realiza en el contexto de la autenticación dependiendo el departamento o cargo correspondiente.

Integridad

Es la seguridad de que la información entrante es la misma que la que se ha enviado. Para entender la integridad, primero se debe comprender los conceptos de integridad de los datos e integridad del sistema de la organización.

Integridad de los Datos

los datos están protegidos contra cambios o manipulaciones no autorizados. La integridad de los datos los defiende contra riesgos de seguridad como la manipulación, donde alguien intercepta y modifica la información sin estar autorizado para ello. Además de proteger los datos que están almacenados en la red, podría necesitar medidas de seguridad adicionales para garantizar la integridad de los datos cuando estos entran en su sistema procedentes de fuentes que no sean de confianza. Cuando los datos que entran en su sistema proceden de una red pública, se requiere métodos de seguridad para realizar estas tareas:

- Proteger los datos para que no se puedan husmear ni interpretar, lo que se suele hacer cifrándolos.
- Asegurar que las transmisiones no han sido alteradas (integridad de los datos).
- Demostrar que se ha producido la transmisión (no repudio). En el futuro, es posible que necesite el equivalente electrónico del correo certificado.

Integridad del Sistema

El sistema proporciona resultados coherentes con el rendimiento esperado. En el caso del sistema operativo manejado será multiusuario que, dependiendo el área o departamento y cargos, la integridad del sistema es el componente de seguridad, porque es una parte fundamental de la arquitectura del Sistema Operativo. Por ejemplo, Microsoft Windows**.** De los más populares que existen, inicialmente se trató de un conjunto de distribuciones o entornos operativos gráficos, cuyo rol era brindar a otros sistemas operativos más antiguos como el MS-DOS una representación visual de soporte y de otras herramientas de software. Se publicó por primera vez en 1985 y desde entonces se ha actualizado a nuevas versiones.

Confidencialidad

Es la seguridad de que la información confidencial permanece privada y no es visible para los escuchas intrusos. La confidencialidad es fundamental para la seguridad total de los datos. El cifrado de los datos con certificados digitales y la capa de sockets segura (SSL) o con una conexión de redes privadas virtuales (VPN) permite asegurar la confidencialidad al transmitir datos entre varias redes que no sean de confianza. La política de seguridad debe indicar qué métodos se emplearán para proporcionar la confidencialidad de la información dentro de la red y de la información que sale de ella.

Actividades de Seguridad de Auditoría

Consisten en supervisar los eventos relacionados con la seguridad para proporcionar un archivo de anotaciones de los accesos satisfactorios y de los no satisfactorios (denegados). Los registros de accesos satisfactorios indican quién está haciendo cada tarea en los sistemas. Los registros de accesos no satisfactorios (denegados) indican que alguien está intentando abrirse paso a través de las barreras de seguridad del sistema o que alguien tiene dificultades para acceder al sistema.

Con todos los cambios constantes en tecnología que ocurren en estos días, puede ser un reto permanecer actualizado sobre los consejos de seguridad más recientes y válidos que se deben seguir al navegar sistemas, plataformas, etc. Para la compañía. Las políticas de seguridad identifican las reglas y procedimientos que todas las personas que acceden y utilizan los recursos y activos de la organización deben seguir para obtener grandes resultados.

¿Por Qué es Importante la Seguridad de Datos?

La seguridad de datos es la práctica que consiste en proteger la información digital contra el acceso no autorizado, la corrupción o el robo durante todo su ciclo de vida. Es un concepto

que comprende todos los aspectos de la seguridad de la información, desde la seguridad física del hardware y los dispositivos de almacenamiento hasta los controles administrativos y de acceso, así como la seguridad lógica de las aplicaciones de software. También incluye las políticas y los procedimientos de la organización.

Con el fin de evitar filtraciones de información confidencial de la organización, los contratos firmados a los empleados tendrán clausulas en donde el trabajador se compromete a no dar información importante y relevante a ninguna persona no autorizada.

Las herramientas y las tecnologías de seguridad de datos deben responder a los crecientes desafíos inherentes a la protección de los entornos informáticos complejos, distribuidos, híbridos o multicloud actuales. Por esta razón la organización debe mantenerse a la vanguardia mediante la actualización constante de las herramientas necesarias tales como:

- Herramientas de detección y clasificación de datos. La información confidencial puede residir en repositorios de datos estructurados y no estructurados, como bases de datos, almacenes de datos, plataformas de big data y entornos de cloud. Las soluciones de detección y clasificación de datos automatizan el proceso de identificación de información confidencial, así como la evaluación y la corrección de vulnerabilidades.
- Supervisión de datos y actividades de archivos. Las herramientas de supervisión de actividades de archivos analizan los patrones de uso de datos, lo que permite que los equipos de seguridad vean quién accede a los datos, detecten anomalías e identifiquen riesgos. El bloqueo y las alertas dinámicos también se pueden implementar para patrones de actividades anormales.
- Herramientas de análisis de riesgos y evaluación de vulnerabilidades. Estas soluciones facilitan el proceso de detección y mitigación de vulnerabilidades, como software

obsoleto, configuraciones incorrectas o contraseñas débiles, y también pueden identificar fuentes de datos con un mayor riesgo de exposición.

Para contar con un buen equipo robusto para la recolección de datos lo primero que debe considerarse es la adquisición de equipos de cómputo que permitan cumplir de manera rigurosa con los requisitos y políticas de seguridad establecidos, con el objetivo de consolidar a la organización en el fortalecimiento de su sistema de seguridad informática.

Influencia del Clima Laboral en la Construcción de las Políticas de Seguridad de la Organización

Se analiza a cada individuo que forma parte de la organización, observando su comportamiento y poniendo especial énfasis en aspectos como las emociones, la atención y los estímulos. En este sentido, se estudian los estilos de trabajo de los colaboradores y directivos, así los efectos psicológicos que influyen en la productividad y las condiciones físicas y de seguridad del entorno laboral (Castillo Marín, Benavides Gaviria, & Waltero Vargas, 2019)

(Olaz & Ortiz, El Clima Laboral en la Empresa Familiar, 2014) define tres coordenadas en su intento por definir el significado del clima laboral en atención a sus principales protagonistas: La persona, los grupos y la organización, recoge y amplia en sus formulaciones teóricas vinculándolo a las competencias profesionales con valor de mercado.

Posteriormente (Olaz, El clima laboral en cuestión, 2013) también profundizan en la definición de un modelo de clima laboral, en el que se puede hacer una lectura de influencia auditora al incluir variables de control como son: presión de trabajo, estudio de incidentes y desarrollo de procedimientos, adecuación de estos, comunicación y entrenamiento, nivel de relaciones, políticas de seguridad y procedimientos.

Una de las conexiones que con más frecuencia se observan en la literatura revisada, es la que relaciona el clima laboral con la cultura organizativa. Una primera conexión entre el clima y la cultura viene de la necesidad de captar metodológicamente lo que algunos autores denominaron el "clima colectivo" (Olaz & Ortiz, El Clima Laboral en la Empresa Familiar, 2014) En esta línea de trabajo otros autores (Olaz, El clima laboral en cuestión, 2013) señalan que ya no se trata de insistir en la percepción individual de la "atmósfera" organizativa, también es analizar el producto de la interacción de los individuos, cuyo resultado es este "clima colectivo"; un clima que refleja también un determinado contexto social: el de la organización. Bajo estos elementos varios a considerar encontramos:

En relación con su definición como variable dependiente o independiente de otras tantas, el clima puede considerarse, desde un punto de vista funcional, como variable dependiente de aquellas con las que interactúa tales como: la comunicación, motivación, liderazgo y trabajo en equipo que pueden ir variando su peso explicativo en el transcurso del tiempo, afectando no de igual manera a todos aquellos componentes de la organización.

Es el resultado de un proceso generalmente fraguado en el tiempo y que suele estar influido por las propias inercias culturales de la organización (creencias, comportamientos, valores, visión y códigos éticos).

Puede advertirse como un fenómeno exterior al individuo, no obstante, su grado de percepción puede variar en función de los umbrales de percepción de cada persona, siendo, en ocasiones, divergentes las interpretaciones que pueden hacerse del mismo, esto es, no todo el mundo necesariamente lo percibe de igual modo y manera.

Validar por medio de una encuesta las opiniones de los empleados, áreas y departamentos asociados de la organización a la hora de compactar y desde otra perspectiva el clima también

puede convertirse en variable independiente de otros aspectos relacionados: nivel desempeño, productividad y desarrollo organizativo entre otras. Esta doble perspectiva convierte al clima en efecto y causa a la vez de cuántas relaciones puedan establecerse en un mapa de categorías.

Metodologías de Seguridad Informática

En el campo de la seguridad informática, existen diversas metodologías que orientan a las organizaciones en la identificación, evaluación y gestión de los riesgos que pueden afectar sus sistemas y activos de información. Cada una de ellas propone un enfoque particular para analizar las amenazas y vulnerabilidades, estableciendo procedimientos que facilitan la toma de decisiones y la aplicación de controles adecuados. Entre las metodologías más utilizadas a nivel internacional se destacan OCTAVE, MAGERIT, NIST SP 800-30 e ISO/IEC 27005, las cuales se describen a continuación. (J. Alberts & J. Dorofee, 2007).

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

Fue desarrollada por la Universidad Carnegie Mellon con el propósito de ofrecer una herramienta que permita a las organizaciones evaluar los riesgos desde una perspectiva operacional. Su esencia radica en identificar los activos críticos, las amenazas que los afectan y las vulnerabilidades que pueden ser explotadas. Se caracteriza por ser una metodología cualitativa, enfocada en el análisis organizacional más que en los aspectos técnicos.
Entre sus ventajas se destaca la participación de diferentes áreas de la empresa, lo que genera una visión integral del riesgo. No obstante, su aplicación demanda cierto nivel de madurez institucional y experiencia en gestión de seguridad, por lo cual puede resultar compleja en entornos donde no existe una cultura de seguridad consolidada.

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)

Esta metodología fue creada por el Gobierno de España como una guía formal para la

administración pública, aunque su uso también se ha extendido al sector privado. Propone una estructura cuantitativa, sustentada en catálogos de activos, amenazas y salvaguardas, que permite determinar el impacto y la probabilidad de ocurrencia de los riesgos.

Entre sus fortalezas se encuentra la profundidad del análisis y la claridad de su documentación. Sin embargo, su implementación suele requerir un equipo técnico especializado y una inversión considerable de tiempo, lo que puede dificultar su adopción en organizaciones pequeñas. (Administraciones, 2012)

NIST SP 800-30 (Guide for Conducting Risk Assessments)

El Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) elaboró esta guía con el objetivo de estandarizar la evaluación de riesgos en los sistemas de información federales. Su enfoque es cuantitativo, basado en controles y métricas precisas que facilitan la comparación y priorización de riesgos.

Su principal ventaja radica en la solidez técnica y la precisión de sus lineamientos, ampliamente reconocidos por organismos internacionales. Sin embargo, su estructura formal puede ser demasiado rígida para organizaciones que buscan flexibilidad o que no cuentan con un sistema de gestión de seguridad avanzado. (Technology, 2012)

ISO/IEC 27005:2018

Esta norma internacional complementa la familia ISO 27000, y está directamente alineada con los principios de la ISO/IEC 27001. Define un proceso integral y adaptable para gestionar los riesgos de seguridad de la información, desde su identificación hasta el tratamiento y seguimiento.

Se caracteriza por su flexibilidad y compatibilidad con otros sistemas de gestión, lo que permite integrarla fácilmente en empresas de diferentes tamaños y sectores. Su principal

fortaleza es que ofrece un marco globalmente reconocido, aunque su aplicación requiere disciplina organizacional y compromiso continuo para mantener su efectividad. (ISO/IEC, 2018)

Comparación Y Análisis de Aplicación

Las metodologías mencionadas presentan diferencias en su enfoque y nivel de exigencia.

Tabla 3

Comparación Y Análisis De Aplicación De Metodologías De Seguridad Informática

Metodología	Enfoque principal	Nivel de exigencia	Fortalezas	Debilidades o limitaciones	Nivel de uso actual
OCTAVE	Estratégico y participativo	Medio	Involucra a todas las áreas de la organización; promueve una visión global del riesgo.	Requiere cultura de seguridad consolidada y experiencia previa.	Moderado
MAGERIT	Documental y técnico	Alto	Proporciona análisis detallado y riguroso; ofrece herramientas y catálogos de amenazas.	Compleja y demandante en recursos; menos flexible.	Medio
NIST SP 800-30	Normativo y cuantitativo	Alto	Altamente estructurada y orientada al cumplimiento de estándares internacionales.	Su rigidez puede limitar su adaptación a entornos pequeños o cambiantes.	Muy alto
ISO/IEC 27005	Integral y flexible	Medio-Alto	Compatible con ISO/IEC 27001; adaptable a cualquier tipo de organización.	Requiere compromiso continuo y seguimiento permanente.	Muy alto

Nota. Elaboración Propia

Recomendación para la Organización ECOLOGICAL INNOVA

Teniendo en cuenta el contexto de la empresa ECOLOGICAL INNOVA, su estructura operativa y los objetivos planteados en el Plan director de Seguridad, la metodología que mejor se adapta es ISO/IEC 27005. Esta elección se justifica porque ofrece un marco coherente con la norma ISO/IEC 27001, la cual ya orienta muchas de las prácticas descritas en este trabajo. Su aplicación permitirá fortalecer el proceso de identificación y tratamiento de riesgos, garantizando la mejora continua y la alineación con los estándares internacionales más reconocidos en materia de seguridad de la información.

Objetivo 2

Identificar las amenazas potenciales y las soluciones dentro del marco de la ISO 27001 para mitigar los riesgos y vulnerabilidades identificados en la organización.

Metodología para el Análisis de Riesgos Y Vulnerabilidades Según la Norma ISO/IEC 27001.

El análisis de riesgos constituye una de las actividades esenciales dentro de la gestión de la seguridad de la información. A través de este proceso, la organización logra identificar los posibles eventos que puedan comprometer la confidencialidad, integridad o disponibilidad de sus activos, y establecer mecanismos para prevenirlos o reducir su impacto. (ISO/IEC, 2018)

La norma ISO/IEC 27001, apoyada en las directrices de la ISO/IEC 27005, propone una metodología estructurada que permite evaluar los riesgos de manera ordenada y documentada, garantizando que todas las decisiones se fundamenten en criterios objetivos.

Este proceso se desarrolla en cuatro etapas principales, que abarcan desde la identificación inicial de los riesgos hasta la aplicación de medidas para su control y seguimiento.

a) Identificación de activos, amenazas y vulnerabilidades

El primer paso consiste en elaborar un inventario detallado de los activos que intervienen en el manejo de la información: infraestructura tecnológica, software, bases de datos, redes, documentos físicos y personal que accede o gestiona dichos recursos.

Una vez definidos, se determinan las amenazas que podrían afectarlos —como errores humanos, ataques cibernéticos, fallas eléctricas, accesos no autorizados o desastres naturales—, junto con las vulnerabilidades que podrían facilitar esos incidentes.

Este reconocimiento permite establecer un panorama general del estado de exposición de la organización.

b) Análisis del riesgo

Con los activos y amenazas claramente identificados, se procede a analizar la probabilidad de que cada evento ocurra y el impacto que generaría sobre la operación o la información.

La probabilidad se evalúa considerando la frecuencia o posibilidad de ocurrencia, mientras que el impacto refleja el grado de daño que podría causar, ya sea económico, operativo, reputacional o legal.

Ambos factores se combinan para determinar el nivel de riesgo, de acuerdo con la siguiente relación:

Nivel de Riesgo = Probabilidad × Impacto

Este resultado permite priorizar los riesgos, clasificándolos como altos, medios o bajos, lo cual orienta las acciones de mitigación que deben aplicarse.

c) Evaluación del riesgo.

Durante esta fase, los riesgos se comparan con los criterios definidos por la organización para determinar si son aceptables o requieren intervención inmediata.

Cuando un riesgo supera los límites establecidos, se analiza la mejor alternativa de gestión: reducirlo mediante controles, transferirlo a un tercero (por ejemplo, mediante seguros o contratos), aceptarlo si su efecto es asumible, o evitarlo eliminando la causa que lo origina.

Esta etapa es clave para optimizar los recursos y enfocar los esfuerzos en los aspectos que representan una amenaza real para la continuidad del negocio.

d) Tratamiento y seguimiento del riesgo.

El tratamiento implica diseñar e implementar medidas específicas para mitigar los riesgos identificados. Dichas medidas deben estar alineadas con los controles propuestos en el Anexo A

de la ISO/IEC 27001 (ICONTEC, Sistemas de Gestión de Seguridad de la Información, 2022), el cual aborda aspectos como:

- Definición y aplicación de políticas de seguridad.
- Control de accesos y administración de contraseñas.
- Seguridad física y ambiental en las instalaciones.
- Uso de cifrado y protección de datos sensibles.
- Procedimientos de gestión de incidentes y continuidad del negocio.

Después de aplicar los controles, es indispensable realizar un seguimiento periódico que permita medir su eficacia, detectar nuevos riesgos y actualizar los planes de acción según la evolución tecnológica o los cambios en los procesos internos.

e) Aplicación en la organización ECOLOGICAL INNOVA

En el caso de ECOLOGICAL INNOVA, el análisis de riesgos debe enfocarse en los procesos donde se concentra la información crítica: plataformas de gestión empresarial (CRM y SAP), almacenamiento de datos, accesos a redes internas y servicios en la nube.

El estudio debe considerar amenazas de origen físico, humano y tecnológico, valorando su probabilidad de ocurrencia y el impacto que podrían causar.

Con base en los resultados, se podrán implementar acciones concretas como:

- Restricciones de acceso por niveles de autorización.
- Monitoreo continuo de actividades y registros en los sistemas.
- Políticas de copias de respaldo y recuperación ante incidentes.
- Capacitaciones periódicas sobre buenas prácticas de seguridad.

De esta forma, el procedimiento de análisis de riesgos conforme a la ISO/IEC 27001 garantiza una gestión coherente, verificable y en mejora continua, fortaleciendo la protección de la información y la resiliencia digital de la empresa.

Tabla 4

Análisis de riesgo

Nivel de Probabilidad	Descripción	Valor
Alta	El evento es recurrente o tiene antecedentes comprobados.	3
Media	Existe posibilidad moderada de que ocurra.	2
Baja	Es poco probable que se presente.	1
Nivel de impacto	Descripción	Valor
Alto	Provoca pérdida crítica de información o interrupción grave del servicio.	3
Medio	Afecta parcialmente los procesos o genera retrasos temporales.	2
Bajo	Causa alteraciones menores y fácilmente recuperables.	1

Nota. Tomada de ISO/IEC 27001

Cálculo del nivel de riesgo:

Riesgo = Probabilidad × Impacto

- 1 a 2 → Riesgo bajo
- 3 a 4 → Riesgo medio
- 6 a 9 → Riesgo alto

Nota. Elaboración propia basada en los lineamientos de la norma ISO/IEC 27005:2018.

¿Qué Son?

Las amenazas son las situaciones que desencadenan en un incidente en la empresa, realizando un daño material o pérdidas inmateriales de sus activos de información. El Sistema de Gestión de Seguridad de la Información basado en la ISO 27001 ayuda a controlar las amenazas que pueden desencadenar los incidentes. (ESG Innova Group, 2015)

Hay amenazas de tipo humano, no humanas, humanas internacionales que necesitan de presencia física, humanas internacionales que proceden de origen remoto.

Tabla 5

Amenazas tipo no humano

Amenazas Según Iso 27001 (De Tipo No Humano)	Amenazas Detectadas En La Empresa
Accidentes físicos, industrial como incendios, explosiones, contaminación e inundación.	
Daños físicos o lógicos.	
Accidente por fenómenos naturales, sismo o volcánico.	Deficiencia y conflicto por servicios públicos en el sector donde está ubicada la empresa.
Conflictos y deficiencias en servicios públicos, agua, energía, telecomunicaciones, fluidos y suministros.	
Accidentes de tipo mecánico y electrónico.	

Nota. Elaboración Propia

Solución. Plantas eléctricas robustas, que soportan y abastecen a la empresa en momentos que no hay energía, estabilizadores de energía en las áreas de trabajo.

Tabla 6

Amenazas tipo humano

Amenazas Según Iso 27001 (De Tipo Humano)	Amenazas Detectadas En La Empresa
Error en recogida, transmisión y utilización de datos.	Información confidencial que solo maneja ciertas áreas y se filtran a las que no deberían tener acceso.
Error existente desde el diseño y desarrollo de software.	Errores en software, perdida de información y tiempo de trabajo.
Error en la entrega de información, durante el tránsito y secuencia.	Información como datos de clientes erróneos, desactualizados, falta de trazabilidad y seguimiento.
Errores en seguimiento, monitoreo, trazabilidad y registros de la información.	Bases de datos entregadas a terceros ajenos a la empresa.

Nota. Elaboración Propia

Solución. Se cambia software de trabajo, se hacen pruebas con anterioridad, se adoptan nuevas prácticas por parte de líderes de equipos para el intercambio de información por correo, solo los jefes pueden emitir información de alta complejidad y confidencial, se limitan accesos o permisos a herramientas de trabajo como SAP, CRM SALESFORCE, dependiendo del rol del colaborador. Se realiza seguimiento y se evalúa al equipo SAC en las tareas de actualización y trazabilidad de datos clientes en nuestro CRM. Se ejecuta campaña de actualización de información con documentos tributarios y formularios de uso exclusivo de la empresa que se canaliza solo por comerciales y el área de servicio al cliente. Se bloquea la opción de exportar información masiva como las bases de datos de clientes.

Tabla 7

Amenazas presencia física

Amenazas Según Iso 27001 (Humanas Internacionales Que Necesitan Presencia Física)	Amenazas Detectadas En La Empresa
Acceso físico erróneo mal utilizado.	Accesos poco controlados.
Acceso lógico, pasivo y simple en interacción con la información.	Contraseñas débiles y fáciles de identificar.
Acceso lógico alterado y sustracción de la información transferida, vulnerando la confidencialidad y poderse aprovechar de los bienes y servicios.	Dispositivos sin bloqueo en la ausencia del personal de trabajo, permitiendo que cualquier otro pueda acceder al computador.
Acceso lógico con corrupción, destrucción de la información, la configuración, la integridad del sistema.	Información alterada por personal de trabajo.
Información no disponible por parte del recurso humano.	

Nota. Elaboración Propia

Solución. Practicas de seguimiento por líderes de equipo a cada uno de sus colaboradores con relación a los procesos y la información que comparten. Se retira al personal que se identificó haciendo alteraciones en información. se aplica reuniones, charlas y capacitaciones periódicas por parte de profesionales en seguridad de la información a todas las áreas de trabajo. Se emiten capsulas informativas acerca de las buenas prácticas. Se asignan cursos de seguridad de la información. Se busca integrar y desarrollar actividades que fomenten el apoyo de las áreas en temas de protección de datos, buenas prácticas cibernéticas, adecuado usos de las

herramientas, plataformas, aplicativos para el desarrollo de las funciones en cada roll, se crean manuales, videos e instructivos.

Tabla 8

Amenazas origen remoto

Amenazas Según Iso 27001 (Humana Internacional Que Procede De Un Origen Remoto)	Amenazas Detectadas En La Empresa
Interacción pasiva de cara al acceso lógico.	Información mal direccionada.
Corrupción en el acceso lógico del tránsito de la información y de su configuración.	Perdida de información
Modificaciones en el acceso lógico y transito e la información.	Información confidencial revelada a otros que no deben tener acceso a ella.
Origen e identidad suplantada.	Modificaciones y alteraciones en los procesos para solicitud de información, ya que no lo hacen por medio de los formatos y de manera informal.
Repudio al origen y recepción de la información en tránsito.	

Nota. Elaboración Propia

Solución. Se fortalece y reestructura las políticas de seguridad en la empresa, se comparte a empleados y clientes. Con jefes de áreas se hacen evaluaciones de seguimiento y se proponen indicadores de medida con relación al tránsito de información data compartidas, todos los filtros para entregar información y recibir información deben ser por medio de formatos establecidos por la compañía, revisados y validados, soportados por documentación legal actualizada, toda solicitud de información debe ser de manera formal por correo corporativo, debe quedar registro y trazabilidad de estas solicitudes o procesos en los que se requiere de información en el CRM, con nombres de quienes gestionan la solicitud.

Como solución principal ante estas amenazas según la norma ISO 27001, en la empresa se ha fortalecido el equipo de tecnología, profesionales que han planteado nuevas oportunidades de mejora, que han venido desarrollando proyectos en los que todos los colaboradores se han visto beneficiados y a su vez educados para el buen y correcto uso de las herramientas tecnológicas ya accesos, se volvió requisito del sistema cambiar periódicamente las contraseñas de acceso, tales como mensajes programados que se le generan al personal de trabajo en su equipo de cómputo para el cambio obligatorio de contraseña en las plataformas, aplicativos que se manejan en la empresa.

Se han mantenido capacitaciones constantes las cuales son debidamente evaluadas.

Para el último año se tomó la decisión por gerencia y asesorado por el área de tecnología de IMPLEMENTAR CRM a SALESFORCE y SAP, dos sistemas muy robustos que nos permiten controlar minuciosamente la información, el acceso y tránsito en ellas.

Los accesos a la compañía son con magnetización y tarjeta de acceso portándose en un lugar visible siempre.

Objetivo 3

Desarrollar un plan de acción basado en la norma ISO 27001 para implementar medidas de seguridad efectivas que mitiguen los riesgos y vulnerabilidades identificados en la organización.

Diagnóstico del Estado Actual y Análisis de Brechas

Antes de diseñar un plan de acción en seguridad de la información, es necesario realizar un diagnóstico que permita conocer el estado actual de la organización en relación con los requisitos de la norma ISO/IEC 27001. Este diagnóstico parte de una evaluación documental y práctica de las políticas, procedimientos, controles y responsabilidades existentes en torno a la seguridad de la información.

El propósito de esta fase es identificar las brechas entre la situación real de la empresa y los controles exigidos por la norma, lo que facilita priorizar los aspectos que deben fortalecerse.

En el caso de ECOLOGICAL INNOVA, este análisis debe contemplar aspectos como:

- La existencia de políticas formales de seguridad.
- La asignación de roles y responsabilidades en la gestión de la información.
- Los mecanismos actuales de control de acceso y autenticación.
- La gestión de incidentes, continuidad del negocio y respaldo de datos.
- Las capacitaciones realizadas al personal en temas de ciberseguridad.

Una vez detectadas las brechas, se elabora un informe diagnóstico, en el cual se clasifican los hallazgos por nivel de criticidad (alta, media o baja) y se determinan las áreas que requieren intervención prioritaria.

Definición del Plan de Acción

Con base en el diagnóstico anterior, se diseña el plan de acción para implementar el Sistema de Gestión de Seguridad de la Información (SGSI) bajo los lineamientos de la ISO/IEC 27001. (ISO/IEC, 2018)

El plan debe estructurarse con los siguientes elementos:

- Objetivo General. Fortalecer la seguridad de la información de ECOLOGICAL INNOVA mediante la implementación de controles, políticas y procedimientos alineados con la ISO/IEC 27001.
- Alcance. Aplica a todos los procesos, áreas y sistemas tecnológicos que manejan información crítica o confidencial de la empresa.
- Responsables. Gerencia General, Área de Tecnología, Coordinación de Seguridad de la Información y líderes de procesos.
- Prioridades. Atender de forma inmediata los hallazgos de mayor impacto, especialmente aquellos relacionados con accesos no autorizados, respaldo de información y capacitación del personal.

Cada actividad del plan debe estar asociada a un control específico del Anexo A de la ISO/IEC 27001, de manera que exista una correspondencia directa entre las medidas adoptadas y los requisitos de la norma.

Diseño de Medidas Técnicas, Administrativas Y Operativas

El plan contempla tres tipos de medidas:

- **Técnicas.** Incorporan herramientas y controles tecnológicos para proteger los sistemas de información. Entre ellas se incluyen la segmentación de redes, implementación de firewalls, autenticación multifactor, cifrado de datos y copias de respaldo automatizadas.

- Administrativas. Consisten en la creación o actualización de políticas, procedimientos y reglamentos que regulen el manejo de la información y definan las responsabilidades de los colaboradores. Esto abarca la adopción de políticas de contraseñas seguras, normas de uso de recursos tecnológicos y controles de acceso por rol.
- Operativas. Están orientadas a los procesos diarios de la organización e incluyen la verificación periódica de logs, la revisión de permisos de usuario, la validación de copias de seguridad y la ejecución de pruebas de restauración.

Estas medidas deben documentarse en un Plan Director de Seguridad, el cual servirá como guía práctica para implementar los controles definidos y garantizar la sostenibilidad del sistema.

Estrategia de Implementación

La implementación del plan debe realizarse de forma gradual y controlada, priorizando las acciones que representen mayor beneficio o mitigación de riesgo.

El proceso inicia con la socialización del plan ante los directivos y responsables de cada área, seguida de la capacitación del personal en temas como clasificación de la información, uso seguro de sistemas y prevención de incidentes.

Posteriormente, se procede a la aplicación de los controles técnicos y administrativos, asegurando que todos los cambios sean registrados y validados por el área de tecnología.

Durante la ejecución, se recomienda establecer un cronograma de trabajo con plazos, responsables y recursos asignados, de manera que las acciones puedan ser monitoreadas y evaluadas de forma continua.

Mecanismos de Seguimiento y Evaluación

Para garantizar la eficacia del plan, es indispensable aplicar un proceso permanente de evaluación y mejora continua.

La empresa debe definir mecanismos de control tales como:

Auditorías Internas. Permiten verificar el cumplimiento de las políticas, los procedimientos y los controles implementados.

Indicadores de Desempeño. Miden aspectos como número de incidentes reportados, tiempos de respuesta y nivel de cumplimiento de las acciones correctivas.

Revisiones Periódicas por la Dirección. Aseguran que la alta gerencia conozca los avances, resultados y decisiones derivadas del SGSI.

Acciones de Mejora. se generan a partir de los resultados de las auditorías o de nuevos riesgos identificados, garantizando la actualización constante del sistema.

Estas actividades de seguimiento no solo confirman el grado de cumplimiento de la ISO/IEC 27001 (ESG Innova Group, 2015), sino que también permiten a ECOLOGICAL INNOVA fortalecer su cultura organizacional en materia de seguridad y consolidar un sistema de gestión sostenible en el tiempo.

Conclusión del Plan de Acción

La aplicación de este plan orientado por la norma ISO/IEC 27001 brinda a la organización una hoja de ruta para gestionar sus riesgos de manera proactiva, integrar las medidas técnicas con las administrativas y promover una cultura de seguridad en todos los niveles. El cumplimiento de este enfoque permitirá que ECOLOGICAL INNOVA avance hacia la madurez en su gestión de seguridad de la información, asegurando la protección de sus activos y la continuidad de sus operaciones frente a los desafíos tecnológicos actuales.

En el entorno organizacional actual, donde la información se ha convertido en uno de los activos más valiosos, la protección de los datos y sistemas de la organización es esencial para garantizar la continuidad operativa y la confianza de los stakeholders. Las amenazas cibernéticas, las vulnerabilidades tecnológicas y los riesgos asociados al factor humano representan desafíos significativos que requieren un enfoque extra.

En este contexto, la norma ISO 27001 se posiciona como un marco de referencia internacionalmente reconocido para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Basándose en esta norma, se ha diseñado un plan de acción cuyo objetivo es mitigar los riesgos y vulnerabilidades identificados, fortalecer la postura de seguridad de la organización y garantizar el cumplimiento de los estándares más exigentes en la protección de la información.

El plan propuesto no solo aborda la implementación de controles técnicos y operativos, a su vez pone énfasis en la importancia de las políticas internas, la capacitación del personal y la mejora continua, elementos clave para una gestión integral y sostenible de la seguridad. A través de este enfoque, la organización busca no solo responder a las amenazas actuales, también anticiparse a futuros desafíos, consolidando una base sólida para su desarrollo y resiliencia digital.

Identificación de Riesgos y Vulnerabilidades

Realizar un análisis de riesgos utilizando metodologías reconocidas, como ISO 2700. Priorizar los riesgos.

Cumplimiento de la Norma ISO 27001

Establecer un marco de trabajo basado en la norma ISO 27001, que sirva como guía para definir controles de seguridad especializados.

Asegurar que las medidas propuestas cumplan con los requisitos de un Sistema de Gestión de Seguridad de la Información

Definición de Políticas y Procedimientos

Crear políticas claras y accesibles que definan las responsabilidades de todos los actores involucrados.

Implementar procedimientos estandarizados para la gestión de incidentes, control de accesos, protección de datos y gestión de cambios.

Capacitación y Sensibilización del Personal

Diseñar e impartir programas de capacitación para todos los niveles de la organización, con el objetivo de fortalecer la cultura de seguridad y garantizar que el personal compone la organización.

Seguimiento y Mejora Continua

Implementar mecanismos de monitoreo y evaluación, como auditorías internas y externas, para verificar la efectividad de las medidas adquiridas.

Utilizar los resultados obtenidos para ajustar y optimizar el plan de acción, asegurando la adaptación a nuevos desafíos y la alineación constante con la norma ISO.

Conclusiones

En el marco de esta monografía, se puede concluir que la empresa ECOLOGICAL INNOVA se encuentra inmersa en un proceso continuo de mejora en su sistema de seguridad de la información. A través de estrategias efectivas, la organización ha logrado avances significativos, mostrando una respuesta satisfactoria ante la mitigación de problemáticas y amenazas previamente identificadas.

La implementación de nuevas tecnologías de la información ha sido un factor clave en este proceso. Este cambio fue posible gracias a la asesoría de profesionales y personal altamente calificado, quienes aportaron su experiencia para respaldar la toma de decisiones estratégicas y la adquisición de herramientas orientadas a fortalecer la seguridad de la información.

Además, la transición hacia un entorno más seguro ha requerido un esfuerzo conjunto basado en la adaptabilidad, formación y participación activa de las diferentes áreas de trabajo. Este proceso ha puesto de manifiesto la importancia de una reestructuración integral, que incluya la actualización de políticas de seguridad, la optimización de los procesos internos y una redefinición clara de los roles y responsabilidades de los colaboradores.

Referencias Bibliográficas

Administraciones, M. d. (2012). *MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Instituto Nacional de Ciberseguridad (INCIBE).

ANI. (02 de 01 de 2019). *Plan de tratamiento de riesgos de seguridad y privacidad de la información*. https://www.ani.gov.co/sites/default/files/u410/plan_de_tratamiento_de_riesgos_de_seguridad_de_la_informacion_ani.pdf

Arboleda, A. O. (2021). *Propuesta de políticas de seguridad de la información para proteger los activos de información en las organizaciones.* Bogotá: UNAD.

Castillo Marín, B. E., Benavides Gaviria, P. A., & Waltero Vargas, J. P. (2019). *Influencia Del Clima Laboral En El Desempeño Del Colaborador.* Bogotá.

Concepto. (25 de 09 de 2024). *Riesgo*. https://concepto.de/riesgo/

Corporación autonoma regional del valle del cauca. (20 de 03 de 2020). Obtenido de Manual metodología gestión de riesgo seguridad de la información: https://www.cvc.gov.co/sites/default/files/2020-07/MN.0720.03%20V01%2020200320%20Metodologia%20gestion%20de%20riesgo%20seguridad%20de%20la%20informacion.pdf

Correa, J. L. (2017). *Diseño De Un Sgsi (Sistema De Gestión De Seguridad De La Información) Basado En Iso27001 Para Laboratorios Servicios Farmacéuticos De Calidad Sfc Ltda.* Bogotá: UNAD.

Escuela Europea de Excelencia. (2 de 08 de 2024). https://www.escuelaeuropeaexcelencia.com/2019/11/listado-de-amenazas-y-vulnerabilidades-en-iso-27001/

ESG Innova Group. (6 de 4 de 2015). *ISO 27001: Amenazas y vulnerabilidades*. https://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/#:~:text=Las%20amenazas%20son%20las%20situaciones,que%20pueden%20desencadenar%20los%20incidentes

Esginnova Group. (20 de 09 de 2024). https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

Gomez, J. F., & Perez, R. J. (2018). Gestión de Riesgos Empresariales. En *Enfoque en identificar, evaluar y gestionar riesgos en contextos corporativos.* McGraw-Hill.

IBM. (26 de 09 de 2024). *¿Qué es la confiabilidad de los datos?* https://www.ibm.com/mx-es/topics/data-reliability

ICONTEC. (2022). *Sistemas de Gestión de Seguridad de la Información.* Bogotá.

ICONTEC. (2022). Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de Seguridad de la Información. En *NTC-ISO/IEC 27001:2022.* Bogota - Colombia.

ISO/IEC. (2018). *ISO/IEC 27005:2018.* Ginebra: ISO.

J. Alberts, C., & J. Dorofee, A. (2007). *OCTAVE Method Implementation Guide (Version 2.0).* Pittsburgh: Carnegie Mellon University.

Kaspersky. (25 de 09 de 2024). https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

La Superintendencia de Industria y Comercio. (08 de 08 de 2023). *Auditoria*. https://www.sic.gov.co

Olaz, Á. (2013). *El clima laboral en cuestión.* España: Aposta.

Olaz, Á., & Ortiz, P. (2014). *El Clima Laboral en la Empresa Familiar.* España.

Revista Seguridad 360. (16 de 09 de 2024). *Seguridad 360*. https://revistaseguridad360.com/noticias/control-de-accesos/sistemas-de-control-de-acceso-para-empresas-mejora-la-seguridad-y-eficiencia/

Senado de la republica. (27 de 07 de 2023). https://www.senado.gov.co/index.php/documentos/categoria-transparencia/gestion-de-calidad-y-meci/proceso-gestion-de-recursos-tecnologicos/manuales-3/7368-rt-ma02-manual-de-politicas-de-seguridad-de-la-informacion/file

Technology, N. I. (2012). *Guide for Conducting Risk Assessments.* Gaithersburg: (NIST SP 800-30 Rev. 1).

Tecno Seguros. (10 de 02 de 2022). *Tecno Seguros*. https://www.tecnoseguro.com/noticias/casos-de-exito/caso-exito-sistema-control-acceso-suprema-complejo-osong

Apéndices

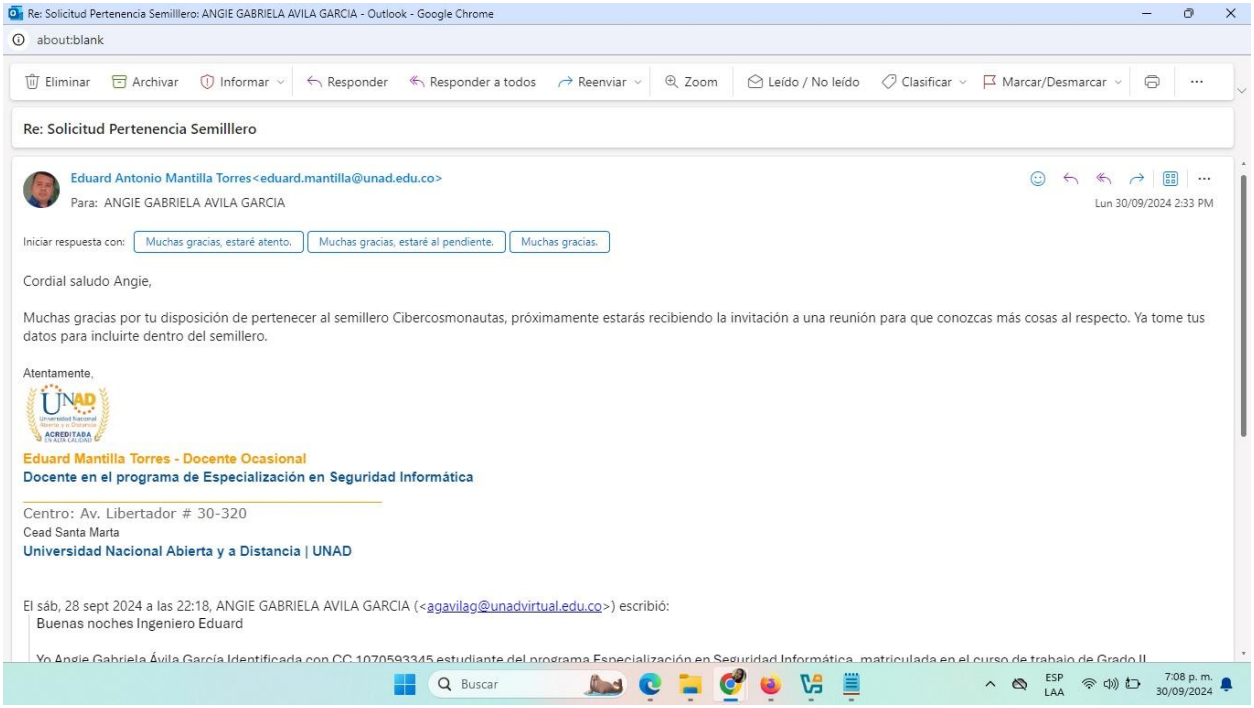
Apéndice A

Video de Socialización Trabajo I

https://unadvirtualedumy.sharepoint.com/:v:/g/personal/agavilag_unadvirtual_edu_co/EWLVAQO3Tu1Jkg4UzmFuAQAB7Bwq0SGxsOOUax10PKh2Bg?e=8JGzUs

Apéndice B

Solicitud Semillero



Apéndice C

Glosario

CIS

Es una entidad de beneficio social, sin ánimo de lucro, que se rige por las normas del derecho privado.

Copyright

Derechos exclusivos de un autor

Criptografía

Procedimientos descritos en claves, enigmas, cifrados

GAP

Método para evaluar las diferencias entre el desempeño real y el desempeño esperado en una organización o negocio

IEC

Organización de normalización pionera mundial, encargada de preparación de normas internacionales en el ámbito eléctrico de tecnologías.

ISO

Organización Internacional de Normalización, quienes elaboran las normas técnicas internacionales.

NIST

Es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica.

NTC

Componente reductor de temperatura en un aparato tecnológico.

Malversación

Conducta delictiva por apropiación desleal del patrimonio, apropiándose de objetos que hacen parte de dicho patrimonio.

PDS

Plan Director de Seguridad Marca el camino a seguir para alcanzar el nivel de seguridad que nuestra organización necesita. Con el objetivo de facilitar su puesta en marcha.

Sans

Es una institución con ánimo de lucro fundada, Reunir información sobre todo lo referente a seguridad informática.

Vulnerabilidades

El riesgo y su gestión.