UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Sistema de gestión de Control de Accesos basados en la ISO 27001:2013 para proteger la seguridad de información de CV Construcciones Generales SAC

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTOR:

Barrientos Inga, Christian Santos (orcid.org/0000-0001-7593-8675)

ASESOR:

Dr. Necochea Chamorro, Jorge Isaac (orcid.org/0000-0002-3290-8975)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2023

DEDICATORIA

A Dios, por haberme dado la oportunidad de vivir y permitirme alcanzar mi sueño de ser profesional en la carrera que elegí. A mis padres Santos Barrientos & Rocio Inga por darme la base para comenzar en lo que es mi profesión, a mis hermanas Diana Barrientos & Sheyla Barrientos que me apoyaron en todo momento a lograr mis metas. Todos ellos me dieron la confianza y motivación de lograr lo que me propongo.

AGRADECIMIENTO

Agradecer a todas las personas que pasaron y contribuyeron en mi etapa de la universidad y laboral, que me enseñaron a base de su experiencia y conocimiento. Agradecer a mi padre por el apoyo brindado en mi etapa de emprendedor donde lo realice simultáneamente con a la etapa del proyecto de investigación.

ÍNDICE DE CONTENIDOS

CARÁTULA i
DEDICATORIA ii
AGRADECIMIENTO iv
ÍNDICE DE CONTENIDOS v
ÍNDICE DE TABLAS vi
ÍNDICE DE GRÁFICOS v
RESUMEN vi
ABSTRACT vii
I. INTRODUCCIÓN 9
II. MARCO TEÓRICO 14
III. METODOLOGÍA 26
3.1. Tipo y diseño de investigación 27
3.2. Variables y operacionalización 28
3.3. Población (criterios de selección), muestra, muestreo, unidad de análisis 29
3.4. Técnicas e instrumentos de recolección de datos 30
3.5. Procedimientos 31
3.6. Método de análisis de datos 33
3.7. Aspectos éticos 34
IV. RESTULADO 35
V. DISCUSIÓN 48
VI. CONCLUSIONES 51
VII. RECOMENDACIONES 54
REFERENCIAS 57
ANEXO 69

ÍNDICE DE TABLAS

Tabla 1. ISO 27001 - Anexo 9 Control de acceso 36
Tabla 2. Estadísticos descriptivos del indicador de Accesos No Autorizados a la información con el PreTest y Postest 36
Tabla 3. Estadísticos descriptivos del indicador de Información Modificada sin Autorización con el PreTest y Postest 38
Tabla 4. Estadísticos descriptivos del indicador de Inaccesibilidad a la información inmediata con el PreTest y Postest 40
Tabla 5. Prueba Shapiro-Wilk para Accesos no autorizados a la información 42
Tabla 6. Prueba Shapiro-Wilk para Información Modificada sin Autorización 43
Tabla 7. Prueba Shapiro-Wilk para Inaccesibilidad Inmediata a la Información ... 43
Tabla 8. Prueba de T-Student para Accesos no autorizados 44
Tabla 9. Prueba de T de Student para Modificación de información no autorizada 45
Tabla 10. Prueba de T de Student para Inaccesibilidad inmediata a la información 47

ÍNDICE DE GRÁFICOS

Gráfico 1. Histograma del PreTest y PosTest de Accesos no autorizados 37
Gráfico 2. Histograma del PreTest y PosTest de Modificación de información 39
Gráfico 3. Histograma del PreTest y PosTest de Inaccesibilidad de información. 41

RESUMEN

Esta investigación explora la importancia de la información en las empresas, enfatizando la necesidad de preservar su integridad, confidencialidad y disponibilidad para la gestión eficiente de activos de datos. Se centra en cómo un sistema de gestión de control de accesos, conforme a la norma ISO 27001:2013, impacta la seguridad de la información en CV Construcciones Generales SAC. El estudio indaga sobre los efectos de este sistema en los aspectos cruciales de la información empresarial, motivando la investigación desde perspectivas metodológica, teórica y práctica. Se resalta la importancia del resguardo de datos y la necesidad de implementar sistemas de seguridad de la información eficientes.

Utilizando una metodología cuantitativa y pre-experimental, el estudio aplica teoría a un caso práctico. El análisis revela mejoras notables en la seguridad de la información tras la implementación del sistema ISO 27001, destacando una disminución en los accesos no autorizados y los incidentes de inaccesibilidad a la información.

Finalmente, la investigación concluye con análisis utilizando pruebas de Shapiro-Wilk y Wilcoxon, confirmando la normalidad de la distribución y la efectividad del sistema implementado en la mejora de la confidencialidad, integridad y disponibilidad de la información empresarial.

Palabras Clave: Disponibilidad de información, Integridad de información, Confidencialidad de información, control de acceso, seguridad de información.

ABSTRACT

This research explores the importance of information in companies, emphasizing the need to preserve its integrity, confidentiality and availability for the efficient management of data assets. It focuses on how an access control management system, in accordance with the ISO 27001:2013 standard, impacts information security at CV Construcciones Generales SAC. The study investigates the effects of this system on crucial aspects of business information, motivating research from methodological, theoretical and practical perspectives. The importance of data protection and the need to implement efficient information security systems is highlighted.

Using a quantitative and pre-experimental methodology, the study applies theory to a practical case. The analysis reveals notable improvements in information security after the implementation of the ISO 27001 system, highlighting a decrease in unauthorized access and incidents of information inaccessibility.

Finally, the research concludes with analysis using Shapiro-Wilk and Wilcoxon tests, confirming the normality of the distribution and the effectiveness of the implemented system in improving the confidentiality, integrity and availability of business information.

Keywords: Availability of information, Integrity of information, Confidentiality of information, access control, information security.

I. INTRODUCCIÓN

La información juega un rol importante y fundamental en la sociedad actual, independientemente de su origen. Tanto para las empresas como para cualquier entidad, asegurar la precisión de los datos, garantizar la confidencialidad y limitar el acceso a usuarios autorizados son cuestiones críticas. La disponibilidad de información, incluso si es desfavorable, es un factor esencial que no debe subestimarse. Para las empresas, esta importancia se vuelve aún más evidente, ya que están encargadas de gestionar activos de datos valiosos.

Briceño (2021) menciona que el resguardo y cuidado por la información se determina a modo de tareas, las mejores acciones y los procesos aptos destinados a salvaguardar los datos y los softwares del ingreso, uso, divulgación, interrupción, alteración o devastación no permitida. En la actualidad, las organizaciones maduras y en proceso de madurez están implementando la directriz ISO 27001 para garantizar protección de datos sensible y relevante que manejan. La implementación de un sistema fundamentado en este reglamento se ha vuelto común debido a que ayuda a reducir los daños causados por la pérdida o la exposición no autorizada de dicha información por una falencia de autenticación.

Los sistemas de gestión son el ingrediente más relevante de la norma ISO 27001, unificando justificaciones para evaluar las exposiciones a peligros vinculados a la administración de regulación de acceso a los datos institucionales. De la Rosa (2021) resalta que el resguardo actual tiene que ser altamente eficiente y una mejor conciencia de los riesgos ampara a la toma correcta de acciones para que ellos puedan identificarse, evaluarse y mitigar riesgos. Parte de la gestión de la ISO es prevenir el acceso no autorizado y los posibles daños que puedan causar, como la pérdida de información confidencial o la interrupción de las operaciones del negocio.

En Perú, ESET (como se citó en Oblitas, 2021) menciona que muchas empresas en crecimiento no tienen un sistema de seguridad estable para proteger sus recursos. En lo que va de 2021, Perú es el tercer país más lastimado de Latinoamérica y el noveno del mundo con mayor número de ciberataques, sobre todo tras la transición del trabajo en modo presencial a nivel remoto3 Actualmente, el Perú se ha tornado en un blanco importante para los ciberataques, especialmente para las empresas que recién están comenzando a automatizar sus procesos y las

empresas del rubro de construcción no escapan de esta realidad, las organizaciones no están preparadas para abordar las deficiencias de seguridad de manera efectiva. En lugar de adoptar medidas preventivas para proteger su información, se enfocan en medidas reactivas, lo que incrementa la amenaza en términos de finanzas y prestigio. Ahora en una focalización referente a la compañía, la empresa receptora es CV Construcciones Generales SAC, está experimentando un crecimiento constante en la industria constructora de obras en Lima Norte. La falta de protección de datos se ha derivado en una problemática urgente y alarmante para esta organización. La empresa ha sufrido pérdidas financieras significativas, perdiendo licitaciones públicas y privadas debido a la falta de presentación oportuna de propuestas a sus clientes. Esta demora se debe a la falta de disponibilidad de información, lo que ha llevado también a daños en su credibilidad y la desconfianza de los clientes. Además, la divulgación de datos confidenciales en Internet ha afectado gravemente la imagen de la empresa. También se han enfrentado a problemas legales debido a la indiscreción de los empleados en el manejo de la información confidencial. Esta investigación pretende brindar una propuesta de conducta correcta al respeto del resguardo de los activos de datos implementado un sistema de gestión de control de acceso fundamentado en la ISO 27001. Debido a que es pieza esencial para que las organizaciones puedan establecer una estructura y un mayor control de ingreso a sus sistemas.

En este contexto, se formula como cuestionamiento principal lo siguiente: ¿Cómo influye un sistema de gestión de control de accesos basado en la norma ISO 27001:2013 en la seguridad de la información de la empresa CV Construcciones Generales SAC? Además, se tiene tres cuestionamientos específicos: En primer lugar, ¿en qué medida influye un sistema de control de acceso basado en la norma ISO 27001:2013 en la confidencialidad de la información de CV Construcciones Generales SAC? En segundo lugar, ¿cómo afecta un sistema de control de acceso basado en la norma ISO 27001:2013 la integridad de la información de CV Construcciones Generales SAC? Por último, ¿cómo influye un sistema de gestión de control de acceso basado en la norma ISO 27001:2013 en la disponibilidad de la información de CV Construcciones Generales SAC?

La presente investigación se justifica mediante la exposición detallada de las principales razones que motivan su realización.

Para la justificación del desarrollo de esta investigación tenemos el enfoque metodológico donde nos basamos en la relevancia del resguardo de los datos que se destaca en la actualidad, donde los datos se han convertido en recursos invaluables para las organizaciones. La pérdida, sustracción o acceso no autorizado a información confidencial puede acarrear consecuencias significativas, como la disminución de la reputación, posibles implicaciones legales y daños financieros considerables. Por consiguiente, es crucial para CV Construcciones Generales SAC establecer medidas de seguridad robustas para salvaguardar sus datos de manera efectiva; si nos basamos en los requisitos de cumplimiento: dentro de los SGSI se enfoca en preservar la disponibilidad, confidencialidad e integridad incluyendo todos los softwares de procesamiento dentro de la organización. Orellana (2022) indica que los SGSI brinda estrategia y/o soluciones preventivas para mantener intactos los activos de la compañía, ya que la adicción de un sistema de control de accesos direccionados en la directriz es esencial para cumplir con la ISO 27001:2013 específicamente en el Anexo 9 que nos habla de este control. En el contexto particular de CV Construcciones Generales SAC, una pyme del rubro de la construcción, la necesidad de seguridad de la información se hace aún más evidente. La organización maneja datos sensibles relacionados con proyectos, contratos, clientes y empleados, lo que subraya la importancia de instituir un sistema de control de accesos adaptado a sus necesidades específicas. Esto no solo protege los recursos de datos críticos, sino que también refuerza la solidez y confidencialidad de los activos de información en un enfoque empresarial cambiante.

Así mismo, en un enfoque de justificación teórica se sustenta en la necesidad de comprender y aplicar estos principios para lograr una gestión de la seguridad efectiva. El estándar se sustenta en los pilares fundamentales de salvaguarda de los datos, como la confidencialidad, integridad y disponibilidad de los datos, los cuales subyacen en su estructura y son esenciales para proteger la información de organizaciones como CV Construcciones Generales SAC, el control de accesos emerge como un componente esencial en cualquier estrategia de escudo de la

información. Se soporta en teorías de autenticación, autorización y auditoría para asegurar que únicamente individuos con autorización puedan acceder a información y recursos delicados, aspectos fundamentales que son abordados por la ISO 27001 en su enfoque de control de accesos. Esta base teórica sólida proporciona un marco conceptual robusto para la ejecución de un sistema de gestión de control de accesos basado en la directriz ISO 27001 en organizaciones como CV Construcciones Generales SAC.

En base a todo esto, se identifica el objetivo principal: Determinar la forma en que un sistema de gestión de control de accesos basado en la ISO 27001:2013 influye en la seguridad de información de la empresa CV Construcciones Generales SAC. Como objetivos específicos, se busca determinar de qué forma influye un sistema de control de accesos basado en la ISO 27001:2013 en la confidencialidad de información de CV Construcciones Generales SAC, además de determinar de qué forma afecta un sistema de control de accesos basado en la ISO 27001:2013 en la integridad de información de CV Construcciones Generales SAC. Finalmente, se busca determinar de qué forma influye un sistema de control de accesos basado en la ISO 27001:2013 en la disponibilidad de información de CV Construcciones Generales SAC.

Por otro lado como hipótesis principal tenemos: Un sistema de gestión de control de accesos basado en la ISO 27001:2013 mejora la seguridad de información de CV Construcciones Generales SAC y como hipótesis específicos se plantea lo siguiente: un sistema de gestión de control de accesos basado en la ISO 27001:2013 mejora la confidencialidad de información de CV Construcciones Generales SAC, en segunda lugar, un sistema de gestión de control de accesos basado en la ISO 27001:2013 mejora la integridad de información de CV Construcciones Generales SAC y por último, un sistema de gestión de control de accesos basado en la ISO 27001:2013 mejora la disponibilidad de información de CV Construcciones Generales SAC.

II. MARCO TEÓRICO

Se llevó a cabo una minuciosa indagación de términos con el objetivo de examinar datos de fondo y factores que sustenta la investigación. Esta exploración implicó analizar fuentes tanto internacionales como nacionales, centrándose en aspectos como el resguardo de los datos, sistemas de control de protección de la información (SGSI), control de acceso y la directriz 27001. El propósito central de esta revisión fue identificar datos pertinentes que pudieran establecer un fundamento robusto para el estudio y elevar la excelencia de los resultados logrados.

En el trabajo planteado por Paredes y Voto (2021) mostró como meta principal de estudio: identificar la referencia de un conjunto de directrices de resguardo de los datos de la empresa, fundamentado en la directriz 27001:2013, en el control de acceso en compañías que operan con teletrabajo. La variable independiente se identificó como el marco de trabajo de resguardo de la información, mientras que el objeto dependiente fue el control de acceso, que se midió en función de accesibilidad, integridad y disponibilidad. El diseño de este estudio academico fue cuantitativo, con un nivel explicativo-tecnológico, y se implmento mediante un diseño pre-experimental. En su investigación se determinó que la aplicación del marco de resguardo de data según las pautas de las políticas 27001:2013 ha reducido significativamente el índice total de accesos no autorizados a la información en un 27.9%. Inicialmente, este índice se situaba en un 65.4%, disminuyendo posteriormente a un 37.5%.

En el estudio realizado por Aguinaga (2021) la finalidad central del análisis fue identificar el impacto del sistema de gestión apegado a la política 27001 en la protección de la información de una compañía financiera. Para ello, se utilizó el resguardo de la información como objeto dependiente y se identificaron tres criterios: confidencial, integro y disponible. Los hallazgos de la investigación señalan que el resguardo de la información de la entidad financiera ha mejorado significativamente gracias a la instauración de un sistema de control apegado al estándar ISO/IEC 27001:2013. Esto se ha visto reflejado en la rentabilidad del negocio y ha mejorado la comunicación entre las áreas operativas. Se recomienda que futuros trabajos de investigación se realicen de acuerdo con las tendencias actualizadas y el nuevo diseño de la normativa ISO 27001, lo que permitirá una mejor protección de los activos sensibles. La confidencialidad dentro de la

institución financiera se mejoró considerablemente tras la implementación del sistema de gestión. Según los datos recogidos, se registró un aumento del 87.36%, lo que demuestra una mejora del 11.84%. La introducción de esta propuesta resultó en un incremento significativo de la confidencialidad de la información en la entidad.

Similarmente, Risco (2021) en su tesis el propósito general de este análisis fue definir cómo un SGSI conforme en la directriz ISO/IEC 27001 contribuye a la defensa de los datos en la compañía de obra civil Pérez & Pérez SAC, ubicada en Moyobamba, San Martín en el año 2020. La metodología aplicada para recolectar los datos fue la observación de un hecho o fenómeno relacionado con los activos protegidos por el SGSI. Las dimensiones consideradas en el estudio fueron la integridad, confidencial y disponibilidad de la información. Al finalizar la investigación, se encontró que el tanto por ciento de visitas no autorizadas aplicando el sistema de gestión de protección de datos de la constructora Pérez y Pérez SAC decreció significativamente del 68,85% al 15,40%, lo que representa una respuesta positiva del 84,6%. Esto indica que, al implementar una estructura basada en el resguardo de la información, se protegen los bienes de información del acceso no autorizado, donde es primordial la identificación del personal y la validación de ciertos criterios según la disponibilidad tecnológica.

En su investigación, Huerta (2020) se propuso analizar de manera general cómo la puesta en implantación del Sistema de control de protección de la Información contribuye al desarrollo de la gestión de riesgos en Coopsol Consultoría en el año 2019. La investigación fue de tipo cuantitativo y se basó en el reconocimiento de campo mediante la ficha de observación de cada uno de los indicadores, logrando identificar la problemática real en el manejo de riesgos de los bienes de información. El autor concluyó que la ejecución del SGSI tiene un impacto positivo en el método de gestión de riesgos empresariales de Coopsol, según los resultados del estudio. Desde esta perspectiva, se destaca el enfoque positivo que tiene el SGSI en las organizaciones y en su modelo de negocio. Constataron que el uso del sistema de control de resguardo de la información en Coopsol se redujo de manera significativa el porcentaje de virus informáticos. Inicialmente, este porcentaje se encontraba en un 52.60%, disminuyendo notablemente a un 11.40%. Esta mejora se tradujo en un impresionante resultado del 88.05%.

De acuerdo con Cabrera (2018), su objetivo fue crear una guía de directrices enfocado en la directriz ISO 27001 para fortalecer el control del resguardo de los datos. El estudio manejo con un total de 13 participantes, lo que permitió obtener un resultado satisfactorio en la prueba posterior. Como resultado, se concluyó que cada departamento en la organización tiene la responsabilidad de compartir la carga en cuanto a el resguardo de la información. Finalmente, el autor enfatiza la relevancia de los sistemas de control de blindaje de la información para detectar las vulnerabilidades a los que están evidenciados los activos y prevenir el déficit financiero u operacionales. Se determinó que la adaptación del modelo de políticas de resguardo de información guiados en la directriz ISO 27001:2013 logró reducir significativamente el porcentaje total de accesos no autorizados a la información en un 28.3%. Por lo tanto, se puede afirmar con certeza que estas políticas resultaron en una notable disminución del porcentaje total de accesos no autorizados a la data en la Municipalidad en Bongará.

Para Monteza (2019) estableció como objetivo general la elaboración de un Sistema de Control de Custodia de la Información fundamentado en el estándar ISO/IEC 27001:2013 para salvaguardar los bienes de datos relacionados con la recolección y supervisión fiscal de la alcaldía de El Agustino. Los procesos de investigación abarcarón desde la dedicación de los líderes de la empresa hasta la finalización de un manual del SGSI, todo ello con el afán de optimizar la protección de la información en la municipalidad. Se concluyó que, durante el reconocimiento de riesgos relacionados con los recursos de información en el procedimiento de recaudación y fiscalización tributaria del departamento de ingresos, se detectaron varios recursos de información con un riesgo elevado del 44% y un riesgo moderado del 56%. En su conclusión, indicó que la adaptación de un SGSI apegado al estándar 27001 permitió resguardar adecuadamente los bienes de información del área de ingreso e inspección tributaria del área de rentas. Las SGSI garantizan la protección adecuada de los recursos de TI de las áreas de riesgo de la organización, lo que no afecta los procesos del negocio.

Delgado y Vásquez (2019) establecieron como objetivo principal identificar una estructura relacionada con la directriz ISO 27001 para fortalecer la protección informática en la compañía BERENDSON NATACIÓN S.R.L. Para ello, utilizaron la

técnica del cuestionario y como herramienta la encuesta, procesando luego los datos en el software estadístico SPSS. La investigación determinó que el nivel de concienciación del personal de protección de activos en la organización es consistente y que no existen limitaciones en áreas no autorizadas que aceleren la pérdida o robo de datos. Adicionalmente, unas de las conclusiones indicaron que la aplicación de una estructura de Tecnología de la Información (TI) centrada en el resguardo de la información, cimentada en el criterio ISO 27001:2013, logró reducir en un 22% el porcentaje total de información modificada sin autorización. Inicialmente, este índice estaba en un 40.1%,

Arias (2020) en su tesis planteó como meta general detallar los procedimientos requeridos para instaurar la pauta ISO 27001 en el área de TI de la Información de la compañía Esvicac, ubicada en Callao, Perú. Como resultado de su investigación, se obtuvo que la implementación del estándar mejoró notablemente el funcionamiento de la entidad, permitiendo mantener los procesos estables y mejorar la apreciación de los clientes acerca de los servicios brindados. Como conclusión del objetivo general, se establece que la adopción de la normativa ISO 27001 en el departamento de TI de la entidad Esvisac ha mejorado de manera eficaz los procesos existentes y ha reducido el riesgo de la información. En uno de sus metas específicas, se indica que la tasa de vulnerabilidades en los elementos de la estructura de tecnología de la información se disminuyó en un 9,75 % en comparación con la evaluación inicial. Esto contribuye a la seguridad de los dispositivos y a la reducción de los peligros relacionados con los ataques.

Según el estudio realizado por Rodríguez et al. (2020) ha producido resultados significativos que son relevantes para la presente investigación, en la que se propone la adopción de la norma ISO 27001 se presenta como un método eficaz para asegurar el resguardo de la información de los clientes y proveedores. Según el autor, esta norma puede reducir tanto los costos como el tiempo requerido para llevar a cabo los procesos de protección de la información. En relación con la confidencialidad de la información, se destaca la importancia de la discreción en la protección de los activos, lo que se convierte en un componente crítico en la adaptación de decisiones. En cuanto a la disponibilidad y la integridad de los datos, se enfatiza que estas características son cruciales para asegurar el fácil acceso y

la credibilidad de los recursos, especialmente en el marco del incremento en la necesidad de administradores de datos. De acuerdo con el cuarto objetivo específico establecido, se logró una mejora significativa en la confidencialidad organizacional, demostrada por un valor de significancia estadística de 0.000, inferior al umbral de 0.05. En el grupo que inicialmente tenía un nivel deficiente, se observó una reducción del 42.9% en el post-test. Para aquellos en el nivel regular, se registró una mejora del 2.4%, mientras que, en el nivel eficiente, se experimentó un aumento del 40.5%. Estos resultados indican que la información está ahora protegida, ya que no hay registros de usuarios que accedan de manera remota, asegurando así la seguridad de los datos.

Los autores Mayorga y Zapata (2020) condujeron un estudio con la meta de implementar un Sistema de protección de la Información guiado en las praxis ISO/IEC 27001. Para lograr este objetivo, aplicaron una metodología de investigación, indagación y resultados para analizar la información obtenida en el área de TI. Los hallazgos de la investigación señalaron que, además de definir políticas para los usuarios, es igualmente importante aplicarlas a los sistemas de información para poder enfrentar de manera efectiva las múltiples amenazas y vulnerabilidades a las que están expuestos los distintos activos organizacionales. El porcentaje de disponibilidad de la información en sus sistemas administrativos donde se hizo el estudio aumentó a un 95% en contraste con el 39% de disponibilidad inicial.

Por otro lado, Orellana (2022), realizó un estudio cuyo objetivo principal fue la creación de un plan para la ejecución de un SGSI. Para capturar datos, se utilizaron diversas técnicas como asambleas, conferencias y cuestionarios. Los resultados indicaron que la implementación de un SGSI debe enfocarse en políticas que sean aplicables al entorno de negocios de cada organización dando como resultados positivos en términos de diferencias de medias. La media del índice antes de la intervención fue de 96,35, mientras que después de la implementación, aumentó a 98,58. Este hallazgo indica que la variable independiente tuvo un impacto significativo cuando se implementó. Además, el valor mínimo del índice de confidencialidad antes de la intervención fue 82, en comparación con el valor posterior que fue 94. La dispersión del índice de confidencialidad disminuyó del

5.18% al 1.97%. En el caso de CEDIA, en la gran parte de los controles son adaptables. Se concluyó que un SGSI es un sistema que puede adaptarse a cualquier compañía o modelo de negocio.

En su artículo científico publicado, Patiño, Caicedo y Guaña (2019) tuvieron como principio primordial detectar vulnerabilidades y analizar los controles de seguridad enfocados en la eficiencia del acceso a los sistemas y aplicaciones en dos empresas, las cuales no fueron nombradas por motivos de confidencialidad. Los autores concluyeron que en ambas empresas era necesario implementar un proceso oficial para registrar y eliminar los permisos de acceso para cada usuario según su área de pertenencia. Esto se debe a que el grado de madurez de los controles de acceso era poco y se encontraron debilidades en el proceso de gestión de permisos. Los hallazgos revelaron que el modelo de madurez basado en ISM3 demostró su capacidad para evaluar adecuadamente cada componente del modelo sugerido, cumpliendo así con los estándares establecidos por la normativa ISO 27001. La combinación de técnicas como entrevistas, observación y pruebas técnicas, respaldada por herramientas como SqlMap, resultó en una evaluación más precisa. Al aplicar este modelo en ambas empresas, se observó que la Empresa A alcanzó un nivel de madurez clasificado como "Controlado", mientras que la Empresa B fue calificada como "Administrado"

En su tesis, Palma (2019) se propuso diseñar un esquema de seguridad para controlar el acceso a la estructura de red, tomando como dirección la normativa ISO/IEC 27002:2013. Para lograr este objetivo, se analizaron la mayoría de los criterios que se encuentran en el estándar, lo que permitió fortalecer la seguridad de la confidencialidad, disponibilidad e integridad de datos. Como resultado de su estudio, se subsanaron las amenazas potenciales en el sistema del hospital, mejorando así el grado de servicio y su consistencia, lo que previene cualquier problema con los datos manejados ya que a nivel infraestructura el esquema establecido incrementó el nivel de confidencialidad de un 75.52% a un 87.36

En su trabajo de titulación en Ingeniería de Sistemas, Tigse (2020) tuvo como objetivo principal la adaptación de un proyecto de manejo de protección en tecnología de la información fundamentado en el protocolo 27001, con el fin de mejorar la seguridad de los datos en la organización PLASTICAUCHO

INDUSTRIAL S.A. Para capturar los datos necesarios, se utilizaron entrevistas y cuestionarios, adoptando un enfoque cualitativo. Según el cuarto objetivo específico, los análisis descriptivos indicaron que salvaguardar la información resultó en una mejora positiva en su control de seguridad. La prueba de hipótesis reveló un aumento del 83% en el control de seguridad, lo que sugiere que la ejecución de la norma ISO 27001:2013 tiene un impacto significativo en la eficacia del control de seguridad. Durante el análisis inferencial, se empleó la prueba de Wilcoxon y e alcanzó un valor de significancia de 0.000, que es menor al umbral de 0.05, lo que confirma la influencia positiva de la guia ISO 27001:2013 en la administración de resguardo.

En su artículo científico Ruíz, Estrada y Sánchez (2020) se propusieron analizar y desarrollar un patrón adecuado para la manejo de la calidad en el resguardo de la data, utilizando como guía el protocolo ISO/IEC 27001:2013 y aplicándolo en establecimientos educativos. El objetivo final era identificar de manera más fácil los peligros que puedan amenazar la seguridad de los establecimientos de educación superior. Como resultado de su estudio, se pudo comprobar una notable mejora en la protección de la información luego de la aplicación de los mejores procedimientos recomendadas. También antes de la adopción de la praxis ISO 27001 y las medidas de la ISO 27002, el tiempo medio de respuesta frente a un incidente de seguridad era de 42 minutos. No obstante, tras la implementación de todas las medidas, el tiempo de respuesta se redujo a 13 minutos.

Asimismo, Nacipucha (2021) se realizó un estudio cuyo meta principal fue establecer un sistema de gobierno de la protección de datos lineados en la estándar Internacional ISO/IEC 27001:2013 para la entidad ArteHogar S.A. en Ecuador. Se emplearon instrumentos de entrevista para recopilar información y encuesta. Los resultados indicaron que la empresa ArteHogar tiene una disposición real en referencia a la custodia de datos y privacidad, basada en la normativa ISO/IEC 27001:2013. Además, concluyeron que hay una correlación relevante entre el Sistema de Gestión (SGSI) y la categorización de datos valiosos, evidenciada por un coeficiente de correlación de 0.569 y un valor de significancia de p=0.009. En general, este sistema ayuda a prevenir eventos o situaciones que podrían poner en riesgo la información o herramientas valiosas para la organización o el negocio.

Cuellar (2020) realizó una investigación con el propósito de desarrollar un Sistema de Gestión de Resguardo de la Información fundamentado en la praxis ISO/IEC 27001 para la Organización Edutec de los Andes Pitalito. La definición de información como un grupo organizado de recursos que conforman un mensaje fue un aspecto clave en su trabajo. La observación fue utilizada como herramienta para la recopilación de evidencia. Se efectuó un sondeo para evaluar las medidas de seguridad implementadas y encontramos que hay una alta incidencia de virus informáticos que afectan los sistemas y ponen en peligro la información confidencial del instituto. Notaron que no se están utilizando sistemas antivirus con licencia que cumplan con los estándares de seguridad y que las computadoras no están protegidas con UPS. Llegaron a la conclusión de que, al identificar los riesgos de los materiales informativos en las esferas administrativas, se encontraron varios recursos con un alto nivel de riesgo del 44% y un nivel medio del 56%. Por tanto, fue apropiado implementar medidas y controles de seguridad para proteger estos recursos de información. Aunque ningún sistema puede garantizar el resguardo completo de la información, el enfoque de un SGSI según la criterio ISO/IEC 27001 es esencial para monitorear y mitigar los daños potenciales a los dispositivos, sistemas, reputación y continuidad del negocio.

Se finaliza los antecedentes con Mayanquer (2020), en su trabajo de titulación se propuso como punto principal efectuar un estudio sobre la protección de los datos, fundamentado en el protocolo ISO/IEC 27001, para detectar debilidades en la infraestructura informática del departamento de Ingeniería de TI en el campus del Sur de Manabí. En resumen, se encontró que la clase de informática para ingenieros informáticos y de redes carece de los estándares de protección de datos ISO/IEC 27001, que son esenciales para mantener la confidencialidad, integridad y disponibilidad del software de datos y comunicación. A través de su investigación, consiguieron reducir en un 13,55 % la tasa de componentes vulnerables en la infraestructura de TI en comparación con el estado inicial durante la prueba previa. Por lo tanto, se concluye que la implementación de un SGSI es indispensable para fortalecer estas tres características de la información.

A partir de este apartado, se proporcionará una definición clara de las tecnologías y metodologías. También se definirá las dos variables de la investigación.

Para la definición de “sistemas” según Vivar (2019) en su trabajo, un sistema es una colección de partes que participan y se comunican entre sí para lograr una finalidad común. Aunque hay muchos tipos de sistemas, muchos de ellos se pueden representar mediante un estándar que consta de cinco conceptos fundamentales: entradas, salidas, transformación, controles y objetivos.

También se definirá el término "gestión". Según Rubio (2000) en su obra "Introducción a la Gestión Empresarial", la gestión se realiza a través de personas o elementos en grupos de trabajo para lograr metas definidas.

En caso de sistema de gestión Aguinaga (2021) define un sistema de gestión como un conjunto de directrices, reglas y acciones planificadas elaboradas para llevar a cabo un proceso determinado.

La definición de un SGSI de acuerdo con Valencia (2021) menciona que este sistema se compone de políticas, procedimientos, recursos, bienes y acciones relacionadas que son gestionados de manera coordinada por una compañía con el fin de salvaguardar sus recursos de información. Para Briceño (2021) puede definirse como procesos, mejores praxis y normas destinados a defender los datos y los softwares de TI del acceso, uso, detención, exposición, alteración o aislamiento no permitido.

En el ámbito de la información, resulta esencial considerar tres características fundamentales que son de gran importancia. Con el fin de garantizar una correcta administración de la información, se deben tener en cuenta estos aspectos clave que permiten su adecuada manipulación y uso:

En primer lugar, la confidencialidad, que según Samaniego y Ponce (2021) se refiere a la garantía de que solo los usuarios permitidos tengan acceso a la data necesaria para desempeñar sus funciones laborales. Este principio de seguridad asegura la protección contra la exposición de información a personas y sistemas no permitidos, permitiendo que solo aquellos con privilegios y derechos tengan acceso a la información necesaria.

En segundo lugar, la disponibilidad, tal como menciona Valencia (2021) en su libro, hace referencia a permitir que los participantes con permisos accedan a los datos

y los bienes técnicos que necesitan cuando los necesitan en un proceso de negocio en cualquier momento;

Por último, la integridad, que de acuerdo con Briceño (2021), es la capacidad de evitar que nuestros datos se modifiquen de manera no autorizada o no deseada. Esto puede significar la modificación o eliminación no autorizada de algunos o de todos nuestros datos, o también puede referirse a modificaciones no autorizadas, pero no deseadas.

En relación con los Sistemas de Gestión de Seguridad de la Información (SGSI), como por ejemplo un sistema de control de accesos, se utiliza el ciclo de Deming debido a que concede a realizar un monitoreo de los logros obtenidos y reiniciar el proceso desde la primera etapa para lograr una mejora continua. Este proceso, también denominado como el ciclo de optimización continua, se compone de cuatro etapas:

La primera etapa es la “planificación”, según Quiñones (2019), se debe conocer el estado actual de la organización en cuanto a sus procesos y problemas, y se deben establecer un buen cronograma, actividades y responsables para obtener resultados satisfactorios.

En segundo lugar, la “ejecución”, definida por Túquerres (2021), implica la implementación de las funciones definidas en la práctica, con mejoras que se adapten a los cambios en el proceso.

En tercer lugar, la “verificación”, tal como lo indican Carvalho y Marques (2019), se refiere a la comprobación de la implementación del SGSI a través de indicadores de desempeño de cada elemento de control, lo que permite realizar un análisis crítico de las normas de defensa de datos.

Para este estudio investigativo únicamente se consideró el anexo A.9. que habla del control de acceso en base a esta normativa. De acuerdo a Paredes y Voto (2021) donde verificó en la página oficial International Organization for Standardization 2013 indica que es importante elegir una técnica apropiada de verificación de identidad para confirmar la autenticidad del usuario que la reclama. Para lograr una autenticación fuerte y segura, se recomienda utilizar otros métodos

de autenticación que no involucren password, como dispositivos criptográficos, tarjetas inteligentes, fichas o sistemas biométricos. Además, el proceso de inicio de sesión debería organizarse de manera que reduzca al máximo la probabilidad de accesos no autorizados. Con este fin, se debe limitar la información revelada durante el proceso de ingreso al sistema a la mínima necesaria para evitar proporcionar ayuda innecesaria a usuarios no autorizados.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo de investigación

El progreso del análisis está fundamentado en una investigación aplicada. De acuerdo con Ramos (2018), es una herramienta que ayuda a abordar problemas específicos en las organizaciones y a reunir información teórica para adquirir conocimientos de forma fácilmente accesible. Por otro lado, Mejía, Sánchez y Reyes (2018) señalan que la investigación aplicada utiliza el conocimiento adquirido a través de la investigación teórica para encontrar soluciones inmediatas a los problemas.

Enfoque de investigación

Este trabajo se realiza en un enfoque cuantitativo, el cual, según Cárdenas (2018), se compone de información que se puede expresar en términos de datos numéricos y medibles, con el objetivo de obtener resultados precisos y fiables. Este enfoque se caracteriza por utilizar técnicas estadísticas y matemáticas para la evaluación de los datos y la identificacion de las presunciones. Además, permite la realización de mediciones objetivas y comparaciones entre diferentes variables.

Diseño del estudio

El trabajo se desarrolla en la utilización de un diseño experimental de subrama pre-experimental. Según Álvarez (2019), este diseño manipula intencionalmente Al menos un factor causal para determinar su influencia en una o más objetos de estudios resultantes, aunque difiere de los pruebas "originales" en el grado de confiabilidad que se puede obtener del emparejamiento inicial de grupos. Por lo tanto, se utilizará un pre-test como análisis previo y un post-test como análisis posterior para identificar el comportamiento que afecta el uso del instrumento antes y después del procedimiento experimental.

También se trabajó de forma transversal. Según Hernández y Mendoza (2018), se obtienen valores en un instante específico o en un periodo exclusivo, lo que permite evaluar situaciones, fenómenos o eventos en un punto temporal determinado. Se

analiza una incidencia particular y su interrelación con otros factores en un momento, lapso o período específico.

3.2. Variables y operacionalización

Definición Conceptual

Variable Independiente: Sistema de gestión de control de accesos

Como lo menciona Sarango (2020) un sistema de gestión de acceso es un sistema electrónico mediante el cual se controlan las entradas y salidas, lo que nos permite identificar a cada individuo que entra, la hora de entrada y su destino.

Variable Dependiente: Seguridad de la información

De acuerdo con Risco (2021), la evaluación de los procesos, funciones y tareas de la empresa es esencial para analizar la privacidad, integridad y acceso de los valores y activos. La protección de la información se basa en un modelo operativo que puede ser implementado en cualquier proyecto, y está compuesto por un grupo de medidas y técnicas para salvaguardar y gestionar los datos en una compañia.

Definición Operacional

Variable Independiente: Sistema de gestión de control de accesos

Según Paredes y Voto (2021) es una estrategia de seguridad basada en la investigación es un componente esencial de un sistema integral de seguridad que se fundamenta en un análisis de los posibles riesgos empresariales. Posteriormente, se establece, implementa, supervisa, controla, revisa y mejora la protección de la información.

Variable Dependiente: Seguridad de la información

Carrera et al (2019) La protección de la información se refiere a las medidas de prevención y respuesta que deben implementar las entidades, incluyendo políticas, regulaciones, procesos, análisis de riesgos, planes de contingencia y otras medidas para garantizar las dimensiones de información.

3.3. Población (criterios de selección), muestra, muestreo, unidad de análisis

Población

De acuerdo con lo expuesto por Egusquiza (2022), la población se compone de un conjunto de elementos o unidades de análisis disponibles que pertenecen al ámbito de estudio particular en el que se lleva a cabo la investigación. Para esta investigación se define una población de 6 personas que laboran en CV Construcciones Generales SAC en la oficina de Urb. San Felipe – Comas, que harán un registro sobre los incidentes con influencia a la protección de la información con respecto a las dimensiones de confidencialidad, integridad y disponibilidad.

Criterio de inclusión: Para hacer esté análisis solo se tomará en cuenta a los colaboradores del área administrativa y gerencia de la organización con respecto a la oficina ubicada en el distrito de Comas

Criterio de exclusión: No se tomarán en cuenta a los colaboradores de las áreas operativas, esto incluye ingenieros, obreros y personal de limpieza.

Delimitación geográfica: La práctica está enfocada en la empresa CV Construcciones Generales SAC, en la oficina ubicada en la Urbanización San Felipe - Comas

Muestra

Según Hernández y Mendoza (2018), la población se equipará a la muestra cuando el número de individuos que la componen es inferior a cincuenta (50). También definen este tipo de diseño como aquel en el que los grupos o parejas no son seleccionados al azar, sino que se utilizan grupos preexistentes y completos durante el experimento.

De acuerdo a lo mencionado por el autor anterior, al ser nuestra población reducida de 6 usuarios, ya no implicaría realizar una limitación mediante fórmulas, por lo tanto, se tomará la población completa como muestra de la investigación.

Muestreo

En este trabajo se empleó un muestreo de probabilística aleatoria simple seleccionada según criterios específicos y de conveniencia. Todos los datos disponibles en el conjunto principal fueron considerados en la selección, siguiendo un enunciado de criterios homogéneos.

Según la postura presentada por Gaviria (2019), el muestreo probabilístico se caracteriza porque cada individuo del grupo tiene las mismas alternativas en caso de ser elegidos para integrar la muestra, sin que se realicen restricciones o filtros previos.

Para este proyecto la población y muestra serán la misma que una población reducida que no es superior a los 50 registros.

3.4. Técnicas e instrumentos de recolección de datos

Técnica

Para esta práctica la técnica utilizada es el fichaje. De acuerdo con lo afirmado por Torres (2019), el fichaje es una técnica que se emplea para recopilar datos e información de manera organizada, de acuerdo con los criterios y necesidades del

investigador. El fichaje permite al investigador tener una visión general y detallada de los datos recopilados, lo que simplifica la evaluación y la comprensión de los resultados logrados

Instrumento

En este caso, se empleó la ficha de observación, tal como se detalla en el Anexo B adjunto. Dicha ficha será aplicada a la variable dependiente, la cual comprenderá 20 registros correspondientes a las incidencias o eventos relacionados ocurridos durante 20 días laborables. Estos eventos involucraron a los 6 miembros del área administrativa y gerencial. Este instrumento nos permitirá evaluar la confidencialidad mediante la identificación de eventos de acceso no autorizado, analizar la integridad en relación con las incidencias de información modificada sin autorización y evaluar la disponibilidad, teniendo en cuenta la inaccesibilidad inmediata a la información ocasionadas por evento de protección de la información.

De acuerdo con Ñaupas (2018), el fichaje observacional implica recolectar información periódica, válida y confiable sobre el comportamiento y los procesos observados utilizando indicadores que se registran con un cronómetro. La data recolectada se resguarda en una base de datos para proceder con su evaluación.

3.5. Procedimientos

Según lo indicado por Marcano (2018), el procedimiento involucra el cumplimiento de una secuencia de pasos específicos con el fin de llevar a cabo una tarea de manera eficiente y productiva.

El proceso de recopilación de datos fue llevado a cabo meticulosamente, implicando la participación activa de los trabajadores dentro de CV Construcciones Generales SAC. La colaboración de recepcionistas, personal administrativo y los gerentes de la empresa (propietarios) fue fundamental para asegurar perspectivas diversas y una captura exhaustiva de datos.

En la fase inicial, se realizó una presentación detallada, explicando los objetivos de la praxis, las dimensiones específicas y los KPI asignados para cada variable

identificada. Estas dimensiones fueron cuidadosamente alineadas con el tema central de los controles de acceso para la resguardo de la información.

Una vez obtenidas las aprobaciones necesarias de los propietarios de la empresa, se elaboró un plan de acción minucioso. Este plan detalló las actividades a realizar y las herramientas designadas para la recopilación de datos. En este contexto, se eligió SPSS como el software para procesar los datos, asegurando un manejo eficiente y análisis preciso de la información recopilada.

Un paso crucial implicó la formulación de objetivos de investigación bien definidos, que sirvieron como marco guía a lo largo del estudio. Se llevaron a cabo exhaustivas revisiones bibliográficas, explorando diversas fuentes académicas para establecer una sólida base teórica para las indagaciones del estudio. La integración de conocimientos académicos previos enriqueció el proceso de investigación, permitiendo una exploración matizada del tema elegido.

Con la aprobación de los expertos, se implementó la herramienta de observación meticulosamente elaborada. Esta herramienta tenía un historial probado, habiendo sido utilizada con éxito en tesis anteriores referenciadas al resguardo de la Información.

La recopilación de datos fue realizada con la colaboración de la asistente contable, la señorita Rocío Inga, quien debido a su ubicación céntrica en la oficina pudo supervisar todos los equipos y registrar tanto las incidencias como los eventos relacionados con el blindaje de la información. En lo que respecta a la confidencialidad, la asistente registró el acceso al equipo de su compañera por parte del ingeniero de obras y los obreros presentes en la oficina, así como las ocasiones en las que una compañera ingresaba a la sesión de otra utilizando sus credenciales, etc. Estos eventos se registraron como accesos no autorizados. En cuanto a la integridad, se documentaron los informes enviados por correo electrónico entre el personal administrativo y la gerencia, que señalaban retrasos en el alcance del contrato o en la documentación debido a modificaciones no reconocidas y/o eliminaciones no autorizadas. Estos registros se utilizaron como indicadores de eliminación/alteración de datos. Por último, en lo que respecta a la disponibilidad, se registraron eventos como cuentas bloqueadas, pérdida de

servicios o el tiempo necesario para recuperar información valiosa dentro de la organización. Estos eventos se documentaron bajo el indicador de inaccesibilidad de información inmediata.

Al concluir la etapa de recopilación de información, se llevó a cabo un escrutinio riguroso de la información acumulada. Esto implicó un análisis minucioso y una comparación detallada, lo que permitió una interpretación profunda de los resultados. Estos datos y análisis formaron la base sólida sobre la cual se construyeron las conclusiones del estudio, proporcionando una visión comprehensiva y fundamentada sobre el manejo de herramientas de acceso para la custodia de la información en CV Construcciones Generales SAC.

3.6. Método de análisis de datos

Análisis Descriptivo

El actual documento utiliza un análisis descriptivo-comparativo, que incluye tablas de frecuencias simples, diagramas de barras o líneas para presentar los datos. Para Fávero (2019), un análisis descriptivo-comparativo es una técnica utilizada en el trabajo de investigación para describir y comparar características y variables de un conjunto de datos. El análisis descriptivo-comparativo es una técnica valiosa para el trabajo de investigación porque permite al investigador comprender mejor los datos y extraer conclusiones significativas a partir de ellos.

Prueba de Normalidad

Según lo afirmado por Fávero (2019), la prueba de normalidad es un procedimiento que permite determinar la distribución de los datos recabados mediante los análisis realizados. Para llevar a cabo este proceso, existen dos autores que pueden utilizarse dependiendo del parametro de la muestra. Primero, el ejercicio de Shapiro-Wilk se emplea para muestras de 50 individuos o menos, mientras que el test de Kolmogorov-Smirnov se usa para muestras de más de 50 individuos. Después de realizar la prueba, se sigue esta regla: si los niveles de significancia

superan 0.05, se concluye que la diseminación es normal. En caso contrario, se clasifica como no normal o no paramétrica.

Prueba de Hipótesis

Según Galindo (2020) la prueba t de Student es una técnica paramétrica ampliamente empleada en la evaluación comparativa de los promedios de dos grupos distintos, bajo la presunción de normalidad de los datos y el cumplimiento de otras condiciones. En contraste con el ejercicio de los rangos con signo de Wilcoxon, la prueba t de Student se emplea cuando se espera que las muestras sigan una distribución parametrica y los datos se recolectan de manera independiente.

3.7. Aspectos éticos

De acuerdo con lo expuesto por Galindo (2020), es fundamental que un trabajo de investigación siga ciertos principios éticos que satisfagan los requerimientos de la auditoría que se realiza a las publicaciones científicas. Es importante mencionar que estos principios éticos son esenciales para asegurar la honestidad y la claridad en el proceso investigativo. Algunos de los principios éticos que deben cumplirse, abarcan la salvaguarda de las prerrogativas de los participantes en la investigación, la prevención de conflictos de intereses y la veracidad en la presentación de los resultados.

En esta investigación, se ha manejado la información proporcionada por la empresa con un alto grado de confidencialidad, evitando exponer los datos sensibles de la organización.

Es crucial enfatizar que la originalidad y la integridad en la investigación son fundamentales para mantener la credibilidad y el valor del trabajo realizado. El plagio y la falta de citación adecuada pueden llevar a consecuencias graves, como la pérdida de la reputación del investigador o la retirada del trabajo de la publicación científica. Por lo tanto, es importante que los investigadores se comprometan a seguir altos estándares de ética y originalidad en todas las etapas.

IV. RESTULADO

ANÁLISIS DESCRIPTIVO

Para este trabajo de estudio se realizó una evaluación descriptiva de los datos procesados previos y posteriores a la adaptación del sistema de gestión de control de accesos apoyado en la ISO/IEC 27001, con la finalidad de comparar los resultados recolectados en ambos períodos. El objetivo de este paso es evaluar y contrastar el impacto que el sistema ha tenido en el rendimiento de los datos mediante un pretest y postest.

Indicador 1: Porcentaje total de Accesos No Autorizados a la información

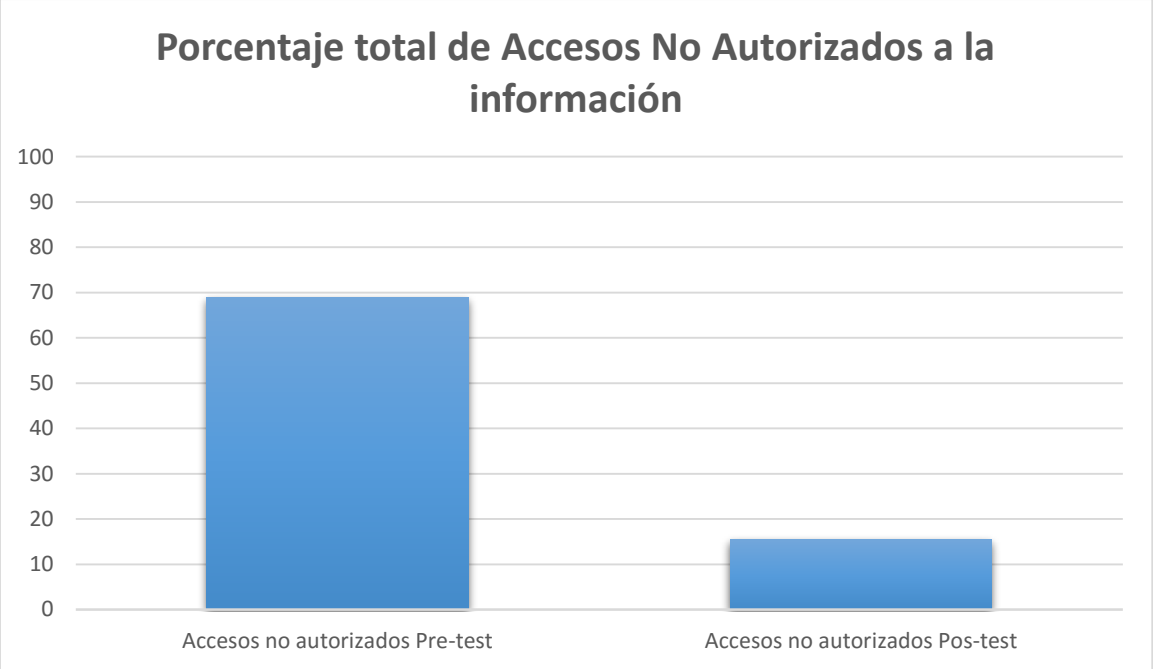
Los resultados descriptivos correspondientes al primer indicador que está basado en la dimensión de la confidencialidad se encuentran disponibles a continuación para la consulta:

Tabla 1. Estadísticos descriptivos del indicador de Accesos No Autorizados a la información con el PreTest y Postest

	N	Min	Max	Media	Desviación estándar	Varianza
Antes de la Implementación	20	45	83	68.85	12.991	168.766
Después de la implementación	20	0	30	15.40	8.165	66.674
Nro. válido por registro 20						

En la tabla 3, se puede observar que, en el Pretest, los accesos no autorizados varían desde 45 hasta 83, con una media de aproximadamente 68.85. Esto indica que, en promedio, los accesos no autorizados estaban en el rango de 68.85 en este periodo inicial. Por otro lado, el Postest, los accesos no autorizados varían desde 0 hasta 30, con una media de aproximadamente 15.40. Esto indica que, en promedio, los accesos no autorizados han disminuido significativamente en comparación con el pretest. Además, la menor desviación estándar y varianza sugieren que los datos están próximos de la media, indicando una mayor consistencia en los resultados.

Gráfico 1. Histograma del PreTest y PosTest de Accesos no autorizados



Como se visualiza en el histograma de la Figura 2, antes de implementar el control de accesos basado en la praxis ISO 27001, aproximadamente el 68.85% de los intentos de acceso no estaban autorizados. Después de implementar el sistema, este número disminuyó significativamente a alrededor del 15.40%. Esta reducción del 53.45% en los intentos de acceso no autorizados muestra la efectividad del sistema en mejorar la confidencialidad y reducir los accesos no autorizados a la información.

Indicador 2: Porcentaje total de Información Modificada sin Autorización

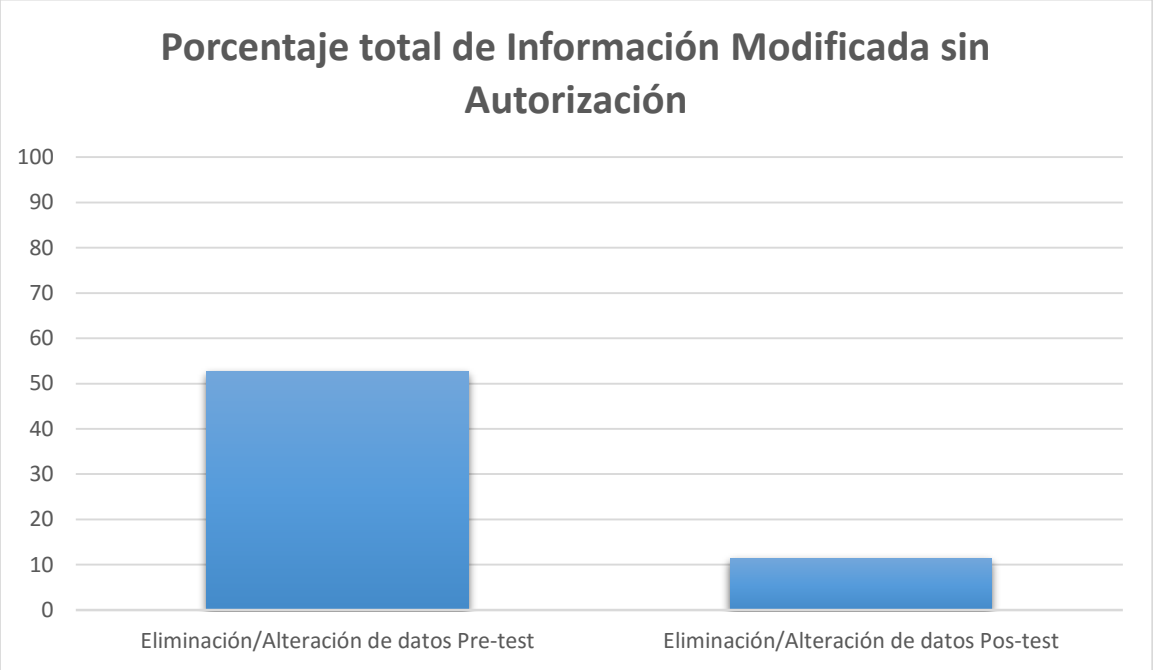
Los resultados descriptivos correspondientes al segundo indicador que está basado en la dimensión de la integridad se encuentran disponibles a continuación para su consulta:

Tabla 2. Estadísticos descriptivos del indicador de Información Modificada sin Autorización con el PreTest y Postest

	N	Min	Max	Media	Desviación estándar	Varianza
Antes de la Implementación	20	40	70	52.60	8.708	75.832
Después de la implementación	20	0	22	11.40	7.287	53.095
Nro. válido por registro 20						

En la tabla 4, se puede observar que, en el pretest, los registros de información modificada sin autorización varían desde 40 hasta 70, con una media de aproximadamente 52.60. Esto indica que, en promedio, una cantidad considerable de información fue modificada sin autorización durante el primer periodo. Pero en la segunda prueba, los registros de información modificada sin autorización varían desde 0 hasta 22, con una media de aproximadamente 11.40. Esto señala que, en términos generales, se visualiza una considerable reducción en la cantidad de información alterada sin permiso en relación con el pretest. La disminución en la desviación estándar y varianza implica que los datos están más centrados en torno a la media, lo que indica una mayor uniformidad en los resultados obtenidos.

Gráfico 2. Histograma del PreTest y PosTest de Modificación de información



Como se observa en el histograma 3, previo a la introducción del sistema de control de accesos conforme a la norma ISO 27001, aproximadamente el 52.60% de los casos mostraban modificaciones no autorizadas en la información. Después de la implementación del sistema, este porcentaje disminuyó significativamente a alrededor del 11.40%. Esta disminución del 41.20% en las alteraciones no autorizadas de la data ilustra la eficacia de la directriz para mejorar la integridad y reducir las modificaciones no permitidas en los datos.

Indicador 3: Porcentaje total de Inaccesibilidad inmediata a la Información

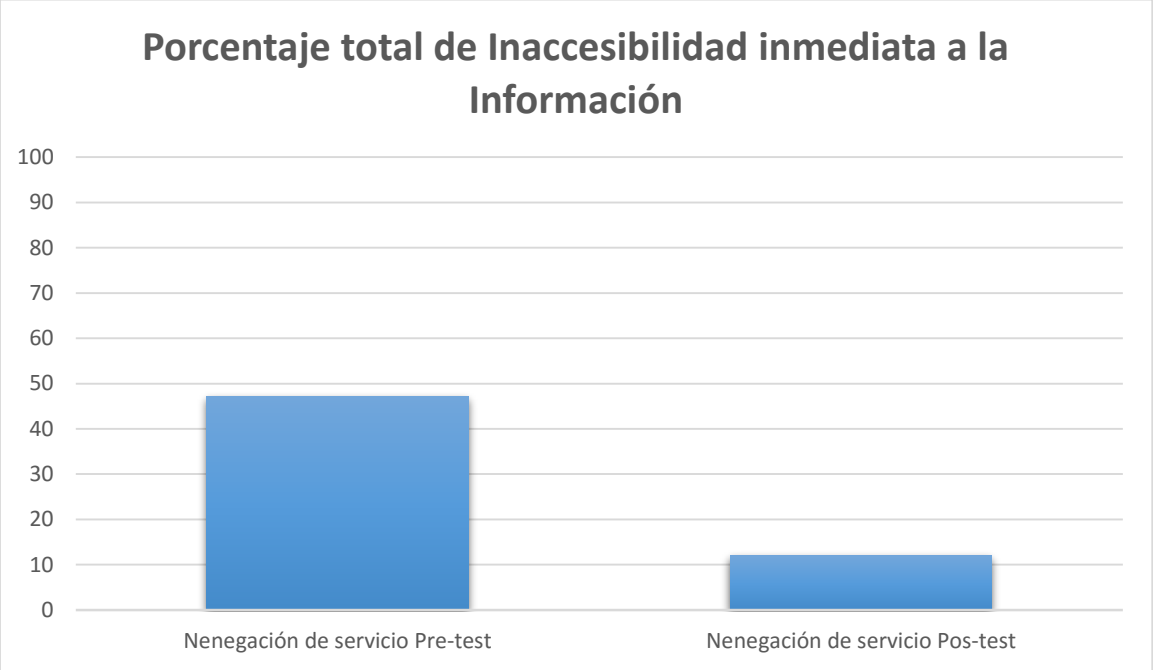
Los resultados descriptivos correspondientes al tercer indicador que está basado en la dimensión de la Disponibilidad se encuentran disponibles a continuación para su consulta:

Tabla 3. Estadísticos descriptivos del indicador de Inaccesibilidad a la información inmediata con el PreTest y Postest

	N	Min	Max	Media	Desviación estándar	Varianza
Antes de la Implementación	20	30	75	47.15	12.419	154.239
Después de la implementación	20	0	29	11.95	9.795	95.945
Nro. válido por registro 20						

Como se puede observar en la tabla 5, en el pretest la disponibilidad inmediata de la información oscilaba entre 30 y 75, con una media cercana a 47.15. Esto señala que, en términos generales, cierta información no pudo ser accesible de inmediato durante ese período inicial. En contraste, en el postest, la accesibilidad inmediata a la información varió de 0 a 29, con una media aproximada de 11.95. Esto indica una mejora considerable en la accesibilidad inmediata a la información en comparación con el pretest. Además, la menor desviación estándar y varianza indican que los datos están próximos alrededor de la media, lo que sugiere una mayor consistencia en los resultados obtenidos.

Gráfico 3. Histograma del PreTest y PosTest de Inaccesibilidad de información



Como se representa en el histograma 4, previo a la adopción del sistema de control de accesos conforme a la norma ISO 27001, alrededor del 47.15% de los incidentes correspondían a la ausencia de disponibilidad inmediata a la información. Después de la aplicación del sistema, este porcentaje experimentó una marcada disminución, alcanzando aproximadamente el 11.95%. Esta disminución del 35.20% en la modificación no autorizada de la información pone de manifiesto la efectividad del método para optimizar de la disponibilidad de la información.

ANÁLISIS INFERENCIAL

Luego de realizar el análisis descriptivo, se procede a realizar el ejercicio de normalidad con el fin de determinar la disposición de los datos obtenidos sigue un patrón normal o no. Esta evaluación es crucial para comprender la naturaleza de los datos y asegurar que los resultados del control de accesos apoyado en la norma ISO 27001 sean confiables y representativos.

Prueba de Normalidad

Smarandache (2020) señala que, al realizar la prueba de normalidad, es fundamental considerar la cantidad de datos recopilados. En casos donde esta cantidad sea de 50 o más, es necesario utilizar el test de Kolmogorov-Smirnov con el fin de establecer el grado de significancia estadística. En concordancia de que la muestra sea diminutiva a 50, se debe utilizar la evaluación de Shapiro-Wilk. Además, si el valor es superior a 0.05, los datos se consideran provenientes de una propagación normal. En contraste, si el valor de significancia es menor a 0.05, se concluye que la propagación no es normal.

Indicador 1: Porcentaje total de Accesos No Autorizados a la información

Se realizaron pruebas de normalidad para el primer indicador “accesos no autorizados a la información” a la diferencia del PosTest con el Pretest.

Tabla 4. Prueba Shapiro-Wilk para Accesos no autorizados a la información

	SHAPIRO-WILK		
	Estadístico	**gl**	**Sig.**
Antes de la implementación – Después de la implementación	,96	20	,53

En la tabla, se puede observar que la información viene de una distribución paramétrica, ya que el significante 0,53, por ende, se utilizará la prueba Tstuden ya que la significancia es un rango mayor al margen de error (a = 0,05)

Indicador 2: Porcentaje total de Información Modificada sin Autorización

Se realizaron pruebas de normalidad para el segundo indicador “Información Modificada sin Autorización” a la diferencia de ambas pruebas (PosTest - PreTest)

Tabla 5. Prueba Shapiro-Wilk para Información Modificada sin Autorización

	SHAPIRO-WILK		
	Estadístico	**gl**	**Sig.**
Antes de la implementación – Después de la implementación	,95	20	,32

Como se observar el segundo indicador, la cantidad de muestra es de un total de 20 registro por lo que se utiliza Shapiro-Wilk, con una significancia superior a 0.05 en la diferencia, se determina que la distribución es normal. En este contexto, la prueba de suposición empleada será el estadístico T-Student.

Indicador 3: Porcentaje total de Inaccesibilidad inmediata a la Información

Se realizaron pruebas de normalidad para el tercer indicador “Inaccesibilidad Inmediata a la Información” aplicado a la resta del Postest y Pretest

Tabla 6. Prueba Shapiro-Wilk para Inaccesibilidad Inmediata a la Información

	SHAPIRO-WILK		
	Estadístico	**gl**	**Sig.**
Antes de la implementación – Después de la implementación	,97	20	,66

Como se visualiza en tabla, el ultimo indicador su significancia es de 0,66 esto sugiere una distribución paramétrica. Por lo tanto, para la evaluación de suposición se utilizará el método T de Student

Prueba de Hipótesis

El estudio, se empleó el procedimiento de T-Student. Conforme a la perspectiva de Caycho, Castillo y Merino (2019), es esencial que los datos experimentales o

muestras utilizadas en las hipótesis cumplan con el requisito de normalidad, incluso si los resultados de la hipótesis son de naturaleza no paramétrica. Este enfoque garantiza la validez y confiabilidad de las conclusiones extraídas del análisis estadístico.

Hipótesis de investigación 1: Prueba de Wilcoxon (No Paramétrica)

Dimensión: Confidencialidad

Hipótesis H1: Un sistema de gestión de control de accesos basado en la ISO 27001:2013 mejora la confidencialidad de información de CV Construcciones Generales SAC

$$H1= x1 > x2$$

Para verificar la hipótesis de investigación 1 de manera rigurosa y precisa, se realizó el análisis correspondiente de rangos con signo de T-Student. Esta elección metodológica se fundamenta en el hecho de que el resultado obtenido se categoriza como no paramétrico o no normal. Para la verificación y análisis de esta prueba Wilcoxon se hará por medio del software IBM SPSS

El criterio de decisión para prueba de hipótesis es la siguiente:

Si la Significancia es < 0.05 La presunción nula es refutada. (H0) y se confirma la suposición alterna (H1)

Tabla 7. Prueba de T-Student para Accesos no autorizados

	Media	Desv. Desviación	Desv. Error Promedio	Margen de error del 95% para la discrepancia		t	gl	Sig. bilateral
				Inferior	Superior			
Antes de la implementación	53.45	15.01	3.36	46.42	60.48	15.92	19	.000

– Después de la implementación								

Para este primer indicador, se puede evidenciar que el nivel de importancia estadística es reducido a 0,05 por lo tanto, se obvia la presunción nula y se confirma la suposición alterna, entonces se afirma qué un sistema de gestión de control de accesos basado en la ISO 27001:2013 mejora la confidencialidad de información de CV Construcciones Generales SAC.

Hipótesis H1: Un sistema de gestión de control de accesos basado en la ISO 27001:2013 mejora la integridad de información de CV Construcciones Generales SAC

$$H1= x1 > x2$$

Para verificar la suposición de investigación 2, se llevó a cabo el test de rangos con signo de T-Student. Esta elección metodológica se fundamenta en el hecho de que el resultado obtenido se categoriza como paramétrico o normal. Para la verificación y análisis de la prueba T-Student se hará por medio del software IBM SPSS

El criterio de decisión para prueba de hipótesis es la siguiente:

Si la Significancia es < 0.05 La presunción nula es refutada. (H0) y se confirma la suposición alterna (H1)

Tabla 8. Prueba de T de Student para Modificación de información no autorizada

	Media	**Desv. Desviación**	**Desv. Error Promedio**	**Margen de error del 95% para la discrepancia**		**t**	**gl**	**Sig. bilateral**
				Inferior	**Superior**			

Antes de la implementación – Después de la implementación	41.20	10.48	2.34	36.30	46.10	17.59	19	.000

Al aplicar un criterio de significancia estadística de cero por ciento, se desestima la presunción nula H0, ya que según el criterio de decisión (0 < 0.05). Por lo tanto, se afirma que un sistema de gestión de control de accesos enfocado en la ISO 27001:2013 mejora la integridad de información de CV Construcciones Generales SAC.

Hipótesis de investigación 3: Disponibilidad

Hipótesis H1: Un sistema de gestión de control de accesos basado en la ISO 27001:2013 mejora la disponibilidad de información de CV Construcciones Generales SAC

$$H1= x1 > x2$$

Con el objetivo de evaluar la hipótesis de investigación 3 con precisión y exhaustividad, se ha implementado el test de Wilcoxon para rangos con signo. La selección de esta metodología se justifica debido a la naturaleza no paramétrica o no normal del resultado obtenido. Para llevar a cabo la verificación y análisis de esta prueba Wilcoxon, se utilizará el software IBM SPSS, garantizando así un enfoque metodológico robusto respaldado por herramientas analíticas especializadas.

El criterio de decisión para prueba de hipótesis es la siguiente:

Si la Significancia es < 0.05 La presunción nula es refutada. (H0) y se confirma la suposición alterna (H1)

Tabla 9. Prueba de T de Student para Inaccesibilidad inmediata a la información

	Media	Desv. Desviación	Desv. Error Promedio	Margen de error del 95% para la discrepancia		t	gl	Sig. bilateral
				Inferior	Superior			
Antes de la implementación – Después de la implementación	35.20	16.88	3.77	27.30	43.10	9.33	19	.000

Para este último indicador, se logra evidenciar que la significancia es inferior a 0,05 por lo tanto, se obvia la presunción nula y se verifica la suposición alterna, entonces se afirma qué un sistema de gestión de control de accesos apoyado en la ISO 27001:2013 mejora la disponibilidad de información de CV Construcciones Generales SAC.

V. DISCUSIÓN

En este apartado se expondrán los resultados del estudio junto con un análisis crítico respaldado por los antecedentes y teorías pertinentes. A continuación, se destacan los contextos previos que se han considerado como los modelos más significativos para la investigación actual.

Aguinaga (2021) ejecuto la aplicación de un sistema de gestión alineado con los estándares estipulados en la normativa ISO/IEC 27001:2013. Su estudio reveló que, mediante el tratamiento de los riesgos de seguridad, se logró una mejora sustancial en la confidencialidad de la información. La ejecución de un Sistema de Gestión de resguardo de la Información (SGSI) resultó en un incremento del 87.36%. En esta investigación, también se observó una mejora significativa en la confidencialidad de los datos, aumentando del 68.85% al 15.40%, lo que representa un aumento del 53%. Estos resultados subrayan que un sistema de gestión de control de accesos apoyado en la ISO 27001:20213 mejora la confidencialidad de información.

En otro estudio, Risco (2021) examinó el desarrollo de un sistema de gestión resguardo de la información conforme a la directriz ISO 27001:2013 en una entidad enfocada en la construcción. La implementación de dicho sistema resultó en una mejora del 41.20% en la integridad de la información de la entidad. En consonancia con estas conclusiones, en el presente proyecto se logró reducir los riesgos asociados a la eliminación y manipulación de datos no validados, garantizando así la integridad de la información. Esta mejora fue notoria, disminuyendo del 52.60% al 11.40%, lo que proporcionó una protección más efectiva de los datos en la empresa CV Construcciones Generales SAC, ya que un sistema de gestión de control de accesos inspirado en la ISO 27001:2013 mejora la integridad de la información.

Finalmente, Paredes y Voto (2021) desarrollaron un marco de trabajo de protección de la información para el control de accesos de usuarios, enfocado y guiado en la normativa ISO/IEC 27001:2013, en empresas de teletrabajo. Su estudio reveló una

disminución significativa del 65.40% al 37.10% en la falta de disponibilidad de la información, representando un mejoramiento del 28.3% tras la implementación. Además, este proyecto logró reducir la indisponibilidad de datos del 47.15% al 11.95%, logrando un resultado favorable del 35.20%. Estos resultados verifican que un sistema de gestión de control de accesos basado en la normativa ISO 27001:20213 mejora la disponibilidad de información.

VI. CONCLUSIONES

Por último, en este estudio se han logrado las siguientes constataciones con el objetivo de determinar los resultados:

En primer lugar, la aplicación del sistema de gestión de control de accesos basado en la normativa ISO 27001:2013 en CV Construcciones Generales S.A.C. ha resultado en una notable mejora en la prevención de accesos no autorizados. El porcentaje de incidencias de accesos no autorizados ha descendido significativamente, pasando de un promedio de 68.85% antes de la implementación a un 15.40% después de la misma. Esto refleja una reducción significativa del 53.45%, reforzando considerablemente la seguridad de la información y la confidencialidad de los datos críticos de la empresa.

Además, los datos reflejados en la investigación revelan una notable disminución en el porcentaje de modificación no autorizada de información, de un 52.60% en el periodo previo a la ejecución del sistema de gestión de control de accesos, a un 11.40% posterior a su aplicación en CV Construcciones Generales S.A.C. Este progreso demuestra una mejora sustancial en la integridad de la información de la entidad que se ve reflejado en una disminución del 41.20% La implementación exitosa de esta estrategia de seguridad ha demostrado ser efectiva para proteger la información crítica de alteraciones indebidas

Adicionalmente, se ha confirmado una significativa mejora, de un 47,15% inicial a un 11,95% posterior, en el porcentaje de inaccesibilidad inmediata a la información gracias al sistema de gestión de control de accesos para el resguardo de la información en CV Construcciones Generales S.A.C. Este avance demuestra la eficacia del sistema en fortalecer las defensas de la empresa contra intentos de interrupción en la disponibilidad de sus servicios y sistemas que se visualiza en una mejora del 35.20%. La reducción de los incidentes de denegación de servicio asegura la continuidad operativa y, por ende, la complacencia del cliente, fortaleciendo el prestigio de la empresa en el ámbito comercial.

Los datos obtenidos revelan que la adaptación del sistema de gestión de control de accesos, conforme a las pautas estipuladas en la normativa ISO 27001, ha asegurado de forma satisfactoria el resguardo de la información en todos los mecanismos de acceso de la compañía CV Construcciones Generales S.A.C. Este logro subraya la eficacia de las prácticas implementadas, evidenciando la firme protección de los datos y confirmando el compromiso de la organización con los estándares de seguridad de renombre internacional.

VII. RECOMENDACIONES

En futuras investigaciones, se sugiere que los investigadores se mantengan actualizados con las últimas tendencias y revisiones de la norma ISO 27001. Dada la evolución constante de las amenazas cibernéticas y los avances tecnológicos, es esencial que cualquier estudio relacionado con la seguridad de la información se base en las prácticas más recientes y relevantes. Al alinearse con estas actualizaciones, las organizaciones pueden estar seguras de que están adoptando las medidas más efectivas para salvaguardar su información corporativa de manera óptima.

Además, se aconseja realizar un análisis exhaustivo de los antecedentes específicos relacionados con las variables y dimensiones vinculadas a la seguridad de la información. Esto implica no solo examinar los casos de estudio existentes, sino también explorar investigaciones y eventos actuales en el ámbito de la ciberseguridad. Un entendimiento profundo de estos antecedentes proporcionará una visión más completa del panorama de la seguridad de la información, permitiendo así una interpretación más precisa y contextualizada de los resultados obtenidos.

Para mejorar la confiabilidad y validez del estudio, es fundamental considerar una amplia gama de indicadores. No limitarse a unas pocas métricas, sino incorporar múltiples variables relevantes, ofrece una visión más holística y detallada del tema en cuestión. Este enfoque enriquecido no solo fortalecerá las conclusiones del estudio, sino que también permitirá identificar patrones y correlaciones que podrían haberse pasado por alto en un análisis más superficial.

Asimismo, se recomienda llevar a cabo una investigación exhaustiva no solo sobre la norma ISO 27001, sino también sobre otras normativas y estándares relacionados, como la NTP/ISO 27001 específicamente adaptada para instituciones financieras. Al profundizar en estas normativas específicas del sector financiero, los investigadores pueden descubrir directrices y requisitos particulares que son esenciales para garantizar la seguridad en entornos financieros altamente

sensibles. Este nivel de detalle es fundamental para desarrollar políticas y prácticas que se alineen no solo con estándares generales, sino también con las necesidades únicas y complejas del sector financiero.

Por último, se sugiere la adaptación integral de la directriz ISO/27001:2013 en la totalidad de las funciones de las instituciones del sector de la construcción. Obtener la certificación internacional a través de esta norma no solo asegura la conformidad con estándares reconocidos a nivel mundial, sino que también genera una mayor confianza entre clientes y proveedores en un mercado altamente competitivo. La certificación internacional no solo representa un logro significativo para la organización, sino que también demuestra un compromiso inquebrantable con la seguridad de la información y la excelencia operativa

REFERENCIAS

AGUINAGA, Quispe. Sistema de gestión alineado a la norma ISO/IEC 27001:2013 para la seguridad de la información en una institución financiera, Chachapoyas-Amazonas, 2021 (Ingeniero de Sistemas). Lima: Universidad Cesar Vallejo, facultad de ingeniería y arquitectura. 2021. 109pp.

ÁLVAREZ, Rafael. Review on the application of virtual reality to vestibular rehabilitation. Ediciones Universidad de Salamanca [en línea]. Julio - agosto 2019, n°. 1. [fecha de consulta: 8 de octubre del 2021]. Disponible en: https://doi.org/10.14201/orl.21215 ISSN 2444-7986

ARIAS, E., 2020. Implementación de la norma ISO 27001 en el Departamento de Tecnología de Información de la empresa Esvicsac, Callao [en línea]. S.l.: Universidad Cesar Vallejo. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/47276/Arias_QES-SD.pdf?sequence=1&isAllowed=y.

BACA, L.S.R., DE LA VEGA, C.F.C.P., CORREDOR, C.M. y DIAZ, M.A.A., 2020. Application of ISO 27001 and its influence on the information security of a Peruvian private company. En: Copyright - © 2020. This work is published under https://creativecommons.org/licenses/bync-nd/4.0/ (the "License"). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License.Última actualización - 2020-12-10, Propositos y Representaciones [en línea], vol. 8, no. 3, pp. 1-11. ISSN 23077999. DOI http://dx.doi.org/10.20511/pyr2020.v8n3.786. Disponible en: https://www.proquest.com/scholarly-journals/aplicación-de-iso-27001-y-suinfluencia-en-la/docview/2468684801/se-2?accountid=37408.

BALAKRISHNAN, Sivaraman. Statistical guarantees for the EM algorithm: From population to sample-based analysis. United State: Project Euclid, Vol. 45 No.1, pp. 77 - 120. Disponible en: https://projecteuclid.org/euclid.aos/1487667618.

BENITEZ, David. REVISIÓN BIBLIOGRÁFICA DE LA NORMA ISO 27001 Y SUS COMPONENTES. (Ingeniero de Sistemas) Tunja: Universidad Santos Tomas, facultad de ingeniería de sistemas. 2019. 78pp. Recuperado en: https://repository.usta.edu.co/bitstream/handle/11634/22099/2016davidbenitez.pdf?seq

BRICEÑO, Edgar Vega. SEGURIDAD DE LA INFORMACIÓN. ALICANTE: ÁREA DE INNOVACIÓN Y DESARROLLO, S.L., 2021. ISBN: 9788412209365

CABRERA, J. Diseño de un modelo de políticas basado en la norma iso 27001, para mejorar la gestión de la seguridad de la información en la municipalidad distrital de Florida. 2018 Bongará – Amazonas. Recuperado el 10 de 02 de 2021, de https://repositorio.upeu.edu.pe/handle/upeu/1542

CAYCHO, C., CASTILLO, C., & Merino, V. (2019). Manual de estadística no paramétrica aplicada a los negocios. Alianza Editorial. Recuperado en : https://hdl.handle.net/20.500.12724/9349

CÁRDENAS, Julián. Investigación cuantitativa. Servicio Alemán de Intercambio Académico: Ministerio Federal de Cooperación Económica y Desarrollo. 2018. 71pp.

CARRERA, F; MACHUCA, S; PALMA, D y SAMPEDRO; C. "PERCEPCION DE SEGURIDAD DE LA INFORMACION EN LAS PEQUENAS Y MEDIANAS EMPRESAS EN SANTO DOMINGO." Investigación Operacional, vol. 40, no. 3, Sept.-Dec. 2019, pp. 421. Gale OneFile: Informe Académico,

link.gale.com/apps/doc/A583252489/IFME?u=anon~5165eb5e&sid=googleScholar&xid=a1a523b2.

CARVALHO, C., & MARQUES, E. Adapting ISO 27001 to a Public Institution. CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Informação) Proceedings, 1– 6. 2019. Recuperado en: http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=1&sid=a7602241-4688-46bf-8a8f-3d05d0b54aba%40sdc-v-sessmgr02

CUELLAR, Jasmín. DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA INSTITUCIÓN EDUTEC DE LOS ANDES PITALITO, ARGUMENTADA EN LA NORMA ISO/IEC 27001 (especialista en Seguridad Informática) Pitalito: Universidad nacional abierta y a distancia UNAD, Escuela de ciencias básicas, tecnología e ingeniería. 2020. 206pp.

DE LA ROSA, Tonysé. AUTOMATION OF AN INFORMATION SECURITY MANAGEMENT SYSTEM BASED ON THE ISO / IEC 27001 STANDARD. Guayaquil: Universidad Metropolitana, 2021. ISSN 2218-3620

DELGADO, Martha y VAZQUEZ, José. MODELO DE SEGURIDAD INFORMÁTICA APLICANDO LA NORMA ISO/IEC 27001 PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN LA EMPRESA BERENDSON NATACIÓN S.R.L. (INGENIERO DE SISTEMAS) Chiclayo: Universidad de Lambayeque, facultad de ciencias de ingeniería. 2019. 127pp.

EGUSQUIZA, Luis. Aplicación móvil utilizando geolocalización para mejorar la Gestión del servicio de traslado de muestras biológicas en la Empresa MJM (Ingeniero de Sistemas) Trujillo: Universidad Cesar Vallejo. 2022. 85pp.

FÁVERO, Luis. Data Science for Business and Decision Making. Academic Press. 2020. Disponible en: https://books.google.com.pe/books?id=ZvKRDwAAQBAJ&pg=PA209&dq=shapiro+wilk+kolmogorov&hl=es-419&sa=X&ved 2ahUKEwj8iciqobjxAhUBhAKHeYaAY4Q6AEwAHoECAcQAg#v=onepage&q=shapiro%20wilk%20kolmogoro v&f=false

FERNÁNDEZ, Víctor. Tipos de justificación en la investigación científica. Espíritu Emprendedor TES. Vol. 4, No. 3. Pag 65-76. 3 de julio 2020. ISSN 2602-8093

FERREIRA, C., PALMEIRA, A., SOUSA, E., AMORIM, C.G., ARAÚJO, A.N. and MONTENEGRO, M.C., 2021. Supramolecular Atropine Potentiometric Sensor. Sensors 2021, Vol. 21, Page 5879 [en línea], vol. 21, no. 17, pp. 5879. DOI 10.3390/S21175879. Disponible en: http://dx.doi.org/10.3390/S21175879.

GALINDO, Hector, ESTADÍSTICA PARA NO ESTADÍSTICOS UNA GUÍA BÁSICA SOBRE LA METODOLOGÍA CUANTITATIVA DE TRABAJOS ACADÉMICOS, marzo 2020. Área de innovación y desarrollo. ISBN: 978-84-121459-3-9

GAVIRIA, Carlos. Estadística descriptiva y probabilidad, editorial bonoaventuriana , 2019.[Consultado 20 de octubre de 2021] 57 Disponible en: https://books.google.com.pe/books?id=YubhDwAAQBAJ&printsec=frontcover&dq=estadistica&hl=es419&sa=X&ved=2ahUKEwjSkJ_s2NrzAhVmIbkGHa8ASU4ChDoAXoECAcQAg #v=onepage&q&f=false

GESTIÓN. Las industrias más expuestas a los ciberataques [en línea]. 14 de junio de 2018. [Fecha de consulta: 20 de octubre 2022]. Disponible:

https://gestion.pe/tecnologia/industrias-expuestas-ciberataques-235985-noticia/

HERNÁNDEZ-SAMPIERI R. y Mendoza, C. Metodología de la investigación: Las rutas cuantitativas, cualitativas y mixta. McGRAW-HILL. 2018. Disponible en: http://virtual.cuautitlan.unam.mx/rudics/wpcontent/uploads/2019/02/RUDICSv9n18p92_95.pdf

HUERTA, Carlos. Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo de Coopsol Consultoría, 2019 (Magister en Ingeniería de Sistemas con mención en Tecnologías de la Información). Lima: Universidad Cesar Vallejo, Escuela de Posgrado. 2020.111pp

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2013. ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements [en línea]. 2013. Suiza: s.n. Disponible en: https://www.iso.org/standard/54534.html.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2013. ISO/IEC 27002:2013 Information technology - Security techniques - Information security management systems - Requirements [en línea]. 2013. Suiza: s.n. Disponible en: https://www.iso.org/standard/68742.html.

MAYANQUER, Javier. ANÁLISIS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS ISO/IEC 27001, PARA IDENTIFICAR VULNERABILIDADES EN LA SALA DE COMPUTO DE LA CARRERA DE INGENIERÍA EN COMPUTACIÓN Y REDES (Ingeniero en cómputo y redes) Manabí: Universidad estatal del sur de Manabí, Facultad de ciencias técnicas. 2020. 118pp.

MAYORGA y Zapata. (2020). Sistema de gestión de seguridad de la información basado en las normas iso/iec 27001, en el departamento de tecnologías de la información del gobierno autónomo descentralizado de la Municipalidad de Ambato. Ecuador. Recuperado el 15 de 02 de 2021, de https://repositorio.uta.edu.ec/jspui/handle/123456789/30694

MARCO & GUIDO. Quality Management: Tools, Methods, and Standards: Vol. First edition. Emerald Publishing Limited. 2019. Recuperado en: http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1949715&lang=es&site=eds-live&ebv=EB&ppid=pp_122.

MARTINEZ, Adriana. IMPORTANCIA DE LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LAS EMPRESAS BAJO LA ISO 27001. Bogotá: Universidad Militar Nueva Granada, facultad de ciencias económica. 2019. 25pp

MEJÍA, Katia, SANCHEZ, Hugo y REYES, Carlos. Manual de términos en investigación científica, tecnológica y humanística. Universidad Ricardo Palma. Lima-Perú. 2018. ISBN Nº 978-612-47351-4-1

MEZA, Robert. Diseño y creación de un sistema identificador de violencia doméstica psicológica por voz. Huancayo: Universidad Continental, Escuela académico profesional de ingeniería de sistemas e informática. 2021. 113pp.

MONTEZA, Lisbet. Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Municipalidad Distrital de El Agustino (Ingeniero de Redes y Comunicaciones). Lima:

Universidad Peruana de Ciencias Aplicadas, facultad de ingeniería. 2019. 370pp.

NACIPUCHA, Julio. ANÁLISIS Y DISEÑO PARA UN MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADOS EN NORMAS ISO/IEC 27001:2013 PARA LA EMPRESA ARTEHOGAR EN LA CIUDAD DE GUAYAQUIL (Ingeniería en sistemas administrativas computarizados) Guayaquil: Universidad de Guayaquil, Carrera de ingeniería en sistemas administrativos computarizados. 2021. 176pp.

ÑAUPAS, H., VALDIVIA, M., PALACIOS, J. and ROMERO, H., 2018. Metodología de la Investigación Cuantitativa - Cualitativa y Redacción de la Tesis. Quinta. Colombia: Ediciones de la U. ISBN 9789587628760.

OBLITAS, Leslie Salas. Diario El Comercio. Ciberataques: Perú es el tercer país más afectado de Latinoamérica en lo que va del año, según Eset. Lima: El Comercio, 2021. https://elcomercio.pe/economia/ciberataques-peru-es-el-tercer-pais-mas-afectado-de-latinoamerica-en-lo-que-va-del-ano-segun-eset-bitcoin-amenazas-informaticas-criptomineros-criptomineria-ncze-noticia/

ORELLANA, María. ELABORACIÓN DE UNA GUÍA DE IMPLEMENTACIÓN DE UN SGSI PARA LA CORPORACIÓN ECUATORIANA PARA EL DESARROLLO DE LA INVESTIGACIÓN Y LA ACADEMIA – CEDIA (Ingeniera de Sistemas). Cuenca: Universidad politécnica salesiana, carrera de ingeniería de sistemas. 2022. 162pp.

PALMA, M., 2019. DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO27002:2013 PARA EL CONTROL DE ACCESO A LA INFRAESTRUCTURA DE RED DE AXXIS

HOSPITAL [en línea]. S.l.: UNIVERSIDAD INTERNACIONAL SEK SER MEJORES. Disponible en: https://repositorio.uisek.edu.ec/bitstream/123456789/3647/1/PALMA AGAMA MARÍA FERNANDA.pdf.

PAREDES, Julio y VOTO BERNALES, Carlos. Marco de trabajo de seguridad de información basado en la ISO/IEC 27001:2013 para el control de acceso de los usuarios en empresas de teletrabajo (Ingeniero de Sistemas). Lima: Universidad Cesar Vallejo, escuela profesional de ingeniería de sistemas. 2021. 145pp.

PATIÑO, S., CAICEDO, A. y GUAÑA, E.R., 2019. Modelo de evaluación del Dominio Control de Acceso de la norma ISO 27002 aplicado al proceso de Gestión de Bases de Datos. En: Copyright - © 2019. This work is published under https://creativecommons.org/licenses/by-nc-nd/4.0 (the "License"). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License.Última actualización - 2021-03-26, Revista Ibérica de Sistemas e Tecnologias de Informação [en línea], no. E22, pp. 230-241. ISSN 16469895. Disponible en: https://www.proquest.com/scholarly-journals/modelo-de-evaluación-deldominio-control-acceso/docview/2317841707/se-2?accountid=37408.

QUIÑONES, Seguil, Aplicación del ciclo PHVA para mejorar la productividad en la fabricación de pernos en Industrias Mendoza S.R.L, Callao - 2019. Recuperado en: https://repositorio.ucv.edu.pe/handle/20.500.12692/45588

RAMOS, Daniel. Desarrollo de Software: Requisitos, Estimaciones y Análisis. 2 edición, Editorial Troy, 2018. [Consultado 21 de abril de 2023] Disponible en: https://books.google.com.pe/books?id=ETuXBgAAQBAJ&printsec=frontcover&dq=scrum&hl=es-419&sa=X&redir_esc=y#v=onepage&q=scrum&f=false

RECALDE, Julia. PLAN DE IMPLEMENTACIÓN DE UN SGSI Y APLICACIÓN DE CONTROLES CRÍTICOS EN EL CENTRO DE OPERACIONES DE SEGURIDAD EN LA EMPRESA GMS (Ingeniera en sistemas informáticos y de computación) Quito: Universidad pública politécnica nacional. 2019. 104pp.

RISCO, Eduardo. Sistema de Gestión para la Seguridad de la Información basado en la Norma ISO/IEC 27001:2013 en la Empresa Constructora Pérez & Pérez SAC, Moyobamba, San Martín,2021 (Ingeniero de Sistemas). Lima: Universidad Cesar Vallejo, facultad de ingeniería y arquitectura. 2021. 118pp.

RODRÍGUEZ, ET AL. (2020). Aplicación de iso 27001 y su influencia en la seguridad de la información de una empresa privada peruana. Lima. Recuperado el 05 de 02 de 2021, de http://www.scielo.org.pe/pdf/pyr/v8n3/2310-4635-pyr-8-03-e786.pdf

RUBIO, Pedro. Introducción a la Gestión Empresarial. Europa: Instituto europeo de Gestión Empresarial. 2000. 297pp. ISBN-10: 8468976024

RUÍZ, J., ESTRADA, C. y SÁNCHEZ, M., 2020. PROPUESTA DE UN MODELO DE UN SISTEMA DE GESTIÓN DE CALIDAD EN SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA INSTITUCIONES EDUCATIVAS. Revista de investgación latinoamericana en competitividad organizacional [en línea], no. 2659-5494, pp. 26. Disponible en: https://www.eumed.net/rev/rilco/05/gestion-instituciones.html.

SAMANIEGO, Eduardo y PONCE, Jessica. Fundamentos de seguridad informática. Guayaquil: Universidad Técnica Estatal de Quevedo. 2021. 110pp. ISBN: 9789942334268.

SARANGO, William. Implementación de control de accesos para mejorar la gestión en seguridad de Hospedaje del Perú SAC. Universidad Cesar Vallejo. Programa académico de maestría en administración de negocios. Chiclayo. 2020. 73pp

SMARANDACHE, Maikel. Neutrosophic Computing and Machine Learning, Vol. 14, 2020. 83pp. ISBN. Disponible en: https://books.google.com.pe/books?id=KSFCEAAAQBAJ&pg=PA73&lpg=PA73&dq=Seg%C3%BAn+Smarandache+(2020)+Shapiro-Wilk&source=bl&ots=zBz8C96kn8&sig=ACfU3U1rzkarPmcr6xkASVz1FfIav8hw-w&hl=es&sa=X&ved=2ahUKEwjI7vzum9z-AhVIIbkGHTaCDhYQ6AF6BAgjEAM#v=onepage&q=Seg%C3%BAn%20Smarandache%20(2020)%20Shapiro-Wilk&f=false

ŠIKMAN, L., LATINOVIĆ, T. y PASPALJ, D., 2019. ISO 27001 - INFORMATION SYSTEMS SECURITY, DEVELOPMENT, TRENDS, TECHNICAL AND ECONOMIC CHALLENGES. En: Copyright - © 2019. This work is published under NOCC (the “License”). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License.Última actualización - 2020-01-24, Annals of the Faculty of Engineering Hunedoara [en línea], vol. 17, no. 4, pp. 45-48. ISSN 15842665. Disponible en: https://www.proquest.com/scholarly-journals/iso-27001-information-systems-security/docview/2344260662/se-2?accountid=37408.

TIGSE, Jorge. PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN EN LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A. (Ingeniero en Sistemas Computacionales e Informáticos) Ecuador: Universidad

Técnica de Ambato, Carrera de Ingeniería en Sistemas, electrónicas e industrial. 2020. 194pp.

TORRES Alvarado, I. D. (2019). El Sistema de Gestión y sus componentes: estratégico, táctico y operacional. Compendium, 22(42), 1–6. Recuperado en: https://revistas.uclave.org/index.php/Compendium/article/view/2555/1547

TORRI, G., GIACOMETTI, R. and PATERLINI, S., 2019. Sparse precision matrices for minimum variance portfolios. Computational Management Science 2019 16:3 [en línea], vol. 16, no. 3, pp. 375–400. DOI 10.1007/S10287-019 00344-6. Disponible en: http://dx.doi.org/10.1007/S10287-019-00344-6

TÚQUERRE, Martínez. Gestión de la calidad con énfasis en el servicio del sector hotelero de la Ciudad de Puyo. Repositorio Universidad Técnica de Ambato: 2021 Recuperado en: https://repositorio.uta.edu.ec/jspui/handle/123456789/32803.

VALENCIA, Francisco. Sistema de gestión de seguridad de la información basado en la familia de normas iso/iec 27000. Bogotá: Universidad Nacional de Colombia. 2021. 181pp. ISBN: 9789587946017

VILLON, Pablo. MODELO DE GESTIÓN DE RIESGOS PARA SEGURIDAD INFORMATICA BAJO ISO/IEC 27001:2013 EN EMPRESA DE ENTRETENIMIENTO Y JUEGOS DE AZAR, LIMA-2021. (Ingeniero de sistemas) Pimentel: Universidad Señor de Sipán. Escuela profesional de ingeniería de sistemas. 2021. 157pp. Recuperado en: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/9215/Villon%20Guerrero%2c%20Pablo%20Leonardo.pdf?sequence=1&isAllowed=y

VIVAR, Marcos. Conceptos y Principios, Fases de los sistemas de información, Análisis de sistemas, diseño de datos, principales características, aplicaciones prácticas (Licenciado en educación Especialidad: Informática) Lima: Universidad nacional de educación, Escuela Profesional de Matemática e Informática. 2019. 69pp.

ANEXO

Anexo 1 Matriz de Consistencia

PROBLEMA	OBJETIVO	HIPOTESIS	OPERACIONALIZACIÓN DE VARIABLES					
			VARIABLE	DIMENSIONES	INDICADORES	MEDICION	ESCALA	METODO
PROBLEMA PRINCIPAL: ¿Cómo influye un sistema de gestión de control de accesos basado en la norma ISO 27001:2013 en la seguridad de la información de la empresa CV Construcciones Generales SAC? **PROBLEMAS SECUNDARIOS:** ¿En qué medida influye un sistema de control de accesos basado en la ISO 27001:2013 en la confidencialidad de información de CV Construcciones Generales SAC? ¿En qué medida afecta un sistema de control de accesos basado en la ISO 27001:2013 en la integridad de información de CV Construcciones Generales SAC? ¿De qué forma influye un sistema de gestión de control de accesos basado en la ISO 27001:2013 en la disponibilidad de información de CV Construcciones Generales SAC?	**OBJETIVO PRINCIPAL:** Determinar la forma en que un sistema de gestión de control de accesos basado en la ISO 27001:2013 influye en la seguridad de información de la empresa CV Construcciones Generales SAC **OBJETIVOS SECUNDARIOS:** Determinar de qué forma influye un sistema de control de accesos basado en la ISO 27001:2013 en la confidencialidad de información de CV Construcciones Generales SAC. Determinar de qué forma afecta un sistema de control de accesos basado en la ISO 27001:2013 en la integridad de información de CV Construcciones Generales SAC. Determinar de qué forma influye un sistema de control de accesos basado en la ISO 27001:2013 en la disponibilidad de información de CV Construcciones Generales SAC.	**HIPÓTESIS PRINCIPAL:** Un sistema de gestión de control de accesos basado en la ISO 27001:2013 mejora la seguridad de información de CV Construcciones Generales SAC. **HIPÓTESIS SECUNDARIOS:** Un sistema de gestión de control de accesos basado en la ISO 27001:2013 mejora la confidencialidad de información de CV Construcciones Generales SAC. Un sistema de gestión de control de accesos basado en la ISO 27001:2013 mejora la integridad de información de CV Construcciones Generales SAC. Un sistema de gestión de control de accesos basado en la ISO 27001:2013 mejora la disponibilidad de información de CV Construcciones Generales SAC.	Sistema de gestión de control de accesos					
			Seguridad de la información	Confidencialidad	Formula: $\mathbf{PTANA} = \frac{\mathbf{ANA}}{\mathbf{AS}} \mathbf{x\ 100}$ Donde: **AS** = Nro. de Accesos al Sistema **ANA**= Nro. de Accesos no autorizados **PTANA**= Porcentaje total de accesos no autorizados a la información	Ficha de Observación	Razón	**Enfoque de la investigación:** Cuantitativa **Tipo de estudio:** Aplicada **Diseño de la investigación:** Preexperimental **Población y muestra:** 6 usuarios **Tipo de muestreo:** Probabilística aleatoria
				Integridad	Formula: $\mathbf{PTIMA} = \frac{\mathbf{IMA}}{\mathbf{IM}} \mathbf{x\ 100}$ Donde: **IM** = Nro. de Información Modificada **IMA** = Nro. de Información Modificada sin Autorización **PTIMA**: Porcentaje total de información modificada sin autorización	Ficha de Observación	Razón	
				Disponibilidad	Formula: $\mathbf{PTINT} = \frac{\mathbf{SINT}}{\mathbf{SAI}} \mathbf{x\ 100}$ Donde: **SAI** = Nro. de Solicitudes de Acceso a la Información **SINT** = Nro. de Solicitudes de acceso a la información interrumpidas **PTINT**= Porcentaje total de inaccesibilidad de la información	Ficha de Observación	Razón	

Anexo 2 Matriz de Operacionalización de variable

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	INSTRUMENTOS DE MEDICIÓN
SISTEMA DE GESTIÓN DE CONTROL DE ACCESOS (INDEPENDIENTE)	De acuerdo con Valencia (2021) un sistema de gestión de control de acceso está compuesto por políticas, procedimientos, recursos, bienes y acciones coordinadas, diseñadas para salvaguardar los valiosos activos de información de una compañía. Estas medidas aseguran que solo las personas autorizadas tengan acceso a la información relevante y necesaria para realizar sus funciones laborales y es esencial para mantener la confidencialidad, integridad y disponibilidad de la información.	Sistema de gestión de control de accesos según Paredes y Voto (2021) es una estrategia de seguridad basada en la investigación es un componente esencial de un sistema completo de gestión de seguridad, que se basa en una un análisis de los posibles riesgos del negocio, para luego establecer, implementar, monitorear, controlar, revisar y mejorar la protección de la información.			
SEGURIDAD DE LA INFORMACIÓN (DEPENDIENTE)	De acuerdo con Risco (2021), la evaluación de los procesos, funciones y tareas de la empresa es esencial para analizar la privacidad, integridad y acceso de los datos. La protección de la información se basa en un modelo operativo que puede ser implementado en cualquier proyecto, y está compuesto por un grupo de medidas y técnicas para salvaguardar y gestionar los datos en una organización.	Carrera et al (2019) La protección de la información se refiere a las medidas de prevención y respuesta que deben implementar las entidades, incluyendo políticas, regulaciones, procesos, análisis de riesgos, planes de contingencia y otras medidas para garantizar la confidencialidad, integridad y disponibilidad de los datos.	Confidencialidad	Porcentaje total de accesos no autorizados a la información	Ficha de Observación
			Integridad	Porcentaje total de información modificada sin autorización	Ficha de Observación
			Disponibilidad	Porcentaje total de inaccesibilidad de la información	Ficha de Observación

Anexo 3

Autorización de la organización para publicar su identidad en los resultados de las investigaciones

UNIVERSIDAD CÉSAR VALLEJO

Anexo

Autorización de la organización para publicar su identidad en los resultados de las investigaciones

Datos Generales

Nombre de la Organización:	RUC: 20503729521
C.V. Construcciones Generales S.A.C	
Nombre del Titular o Representante legal:	
Nombres y Apellidos: Cesar Vargas Zuñiga	DNI: 08105223

Consentimiento:

De conformidad con lo establecido en el artículo 8º, literal "c" del Código de Ética en Investigación de la Universidad César Vallejo (RCU Nro. 0470-2022/UCV) (*), autorizo [X], no autorizo [ ] publicar LA IDENTIDAD DE LA ORGANIZACIÓN, en la cual se lleva a cabo la investigación:

Nombre del Trabajo de Investigación	
SISTEMA DE GESTIÓN DE CONTROL DE ACCESOS BASADO EN LA ISO 27001 DE 2013 PARA PROTEGER LA SEGURIDAD DE INFORMACIÓN DE CV CONSTRUCCIONES GENERALES SAC	
Nombre del Programa Académico: PREGRADO	
Autor: Nombres y Apellidos: CHRISTIAN SANTOS BARRIENTOS INGA	DNI: 71307655

En caso de autorizarse, soy consciente que la investigación será alojada en el Repositorio Institucional de la UCV, la misma que será de acceso abierto para los usuarios y podrá ser referenciada en futuras investigaciones, dejando en claro que los derechos de propiedad intelectual corresponden exclusivamente al autor (a) del estudio.

Lugar y Fecha:

CV CONSTRUCCIONES GENERALES S.A.C

Firma: _____

Cesar Vargas Zuñiga
GERENTE GENERAL

(Titular o Representante legal de la institución)

(*) Código de Ética en Investigación de la Universidad César Vallejo-Artículo 8º, literal "c" **Para difundir o publicar los resultados de un trabajo de investigación es necesario mantener bajo anonimato el nombre de la institución donde se llevó a cabo el estudio, salvo el caso en que haya un acuerdo formal con el gerente o director de la organización, para que se difunda la identidad de la institución. Por ello, tanto en los proyectos de investigación como en las tesis, no se deberá incluir la denominación de la organización, ni en el cuerpo de la tesis ni en los anexos, pero sí será necesario describir sus características.**

de tesis.

Anexo 4

Permiso de Publicación de la Tesis

CV CONSTRUCCIONES GENERALES S.A.C

Lima, 13 de noviembre del 2023

A quien corresponda:

Por la presente CV CONSTRUCCIONES GENERALES S.A.C, representada por Cesar Vargas Zúñiga en su calidad de Gerente General, otorga su consentimiento formal para que la tesis realizada por Christian Barrientos Inga, titulada "Sistema de Gestión de Control de Accesos basado en la ISO/IEC 27001 para proteger la seguridad de información de CV CONSTRUCCIONES GENERALES S.A.C., sea publicada y compartida en el repositorio académico de la Universidad Cesar Vallejo.

Reconocemos el valor de compartir conocimientos y resultados de investigación con la comunidad académica y estamos de acuerdo en que los hallazgos presentados en la tesis pueden ser de interés público para el avance científico y tecnológico.

Por medio de este documento, confirmamos que no hay restricciones de confidencialidad o derechos de autor que impidan esta publicación y que cualquier información sensible ha sido debidamente anonimizada o excluida del documento a publicar.

Este permiso se otorga sin perjuicio de los derechos propietarios de CV CONSTRUCCIONES GENERALES S.A.C. y con el entendimiento de que los créditos y reconocimientos apropiados se otorgarán a la empresa en la publicación de la tesis.

Atentamente,

CV CONSTRUCCIONES GENERALES S.A.C.

Cesar Vargas Zúñiga
GERENTE GENERAL

Firma del Gerente General

Anexo 5

Carta de Compromiso de la Empresa

CV
CONSTRUCCIONES
GENERALES S.A.C

Lima, 13 de noviembre del 2023

Por medio de la presente, CV CONSTRUCCIONES GENERALES S.A.C. representada por Cesar Vargas Zúñiga siendo Gerente General, se compromete formalmente a brindar apoyo integral al estudiante Christian Barrientos Inga de la carrera de Ingeniera de Sistema en de la Universidad Cesar Vallejo, quien está desarrollando el proyecto de tesis titulado Sistemas de Gestión de Control de Acceso basado en la ISO 27001 para proteger la seguridad de la información de CV COSTRUCCIONES GENERALES SAC.

Nos comprometemos a:

- Proporcionar información relevante y específica que sea necesaria para el desarrollo y la culminación exitosa del proyecto de tesis.
- Facilitar el acceso a nuestras instalaciones, recursos y personal técnico que puedan contribuir con su experiencia y conocimiento al progreso del proyecto.
- Brindar asesoría técnica y apoyo logístico que sean requeridos durante el período del proyecto.

Entendemos la importancia de la colaboración entre el sector empresarial y académico para el fortalecimiento del conocimiento y la innovación. Por ello, reiteramos nuestro compromiso de apoyar a Christian Barrientos Inga en cada etapa de su proyecto de tesis realizada en la empresa siempre y cuando ello no afecte la integridad y reputación de la organización.

Atentamente,

CV CONSTRUCCIONES GENERALES S.A.C
Cesar Vargas Zúñiga
GERENTE GENERAL

Firma del Gerente General

Anexo 6

Acuerdo de Publicación en Revistas de Investigación

CV CONSTRUCCIONES GENERALES S.A.C

Lima, 13 de noviembre del 2023

Representante Legal: Cesar Vargas Zúñiga
Fecha: 13/11/2023

Por medio del presente, CV CONSTRUCCIONES GENERALES S.A.C. autoriza a Christian Barrientos Inga a someter su tesis titulada "Sistema de Gestión de Control de Acceso basado en la ISO/IEC 27001 para proteger la seguridad de la información de CV CONSTRUCCIONES GENERALES S.A.C." para su revisión y consideración de publicación en revistas de investigación académicas.

La empresa confirma que el material presentado no contiene información confidencial y puede ser divulgado a la comunidad científica.

Atentamente,

CV CONSTRUCCIONES GENERALES S.A.C.
Cesar Vargas Zúñiga
GERENTE GENERAL

Firma del Gerente General

Anexo 7

Documento de Capacitaciones al Personal con el Nuevo Sistema

CV CONSTRUCCIONES GENERALES S.A.C

Lima, 13 de noviembre del 2023

Empresa: CV CONSTRUCCIONES GENERALES S.A.C.
Representante Legal: Cesar Vargas Zúñiga
Fecha: 13/11/2023

El presente documento certifica que se han llevado a cabo las siguientes sesiones de capacitación para el personal con respecto al Sistema de Gestión de Control de Accesos basado en la ISO/IEC 27001:2023 para proteger la seguridad de información en CV CONSTRUCCIONES GENERALES S.A.C:

CONOCIMIENTO PREVIO DE LA ISO/IEC 27001
Fecha: 01/08/2023
Duración: 1 Hora
Contenido: Visión general de la ISO/IEC 27001:2013
Concepto principales y manejo de contraseña robusta

CAPACITACIÓN DEL SISTEMA DE GESTIÓN DE CONTROL DE ACCESO BASADO EN LA ISO/IEC 27001
Fecha: 02/10/2023
Duración: 2 Horas y 30 media
Contenido: Manejo del Sistema de Gestión de control de Accesos

Las capacitaciones se han impartido con el objetivo de asegurar que el personal maneje el sistema de manera eficiente, manteniendo la productividad y la seguridad de la información de la organización

CV CONSTRUCCIONES GENERALES S.A.C
Cesar Vargas Zúñiga
GERENTE GENERAL
Firma del Gerente General

Anexo 8

Certificación de Implementación del Sistema en la Empresa

CV CONSTRUCCIONES GENERALES S.A.C

Lima, 13 de noviembre del 2023

Por medio de la presente, CV CONSTRUCCIONES GENERALES S.A.C. representada por Cesar Vargas Zúñiga siendo Gerente General, certifica que el Sistema de Gestión de Control de Acceso basado en la ISO 27001 ha sido exitosamente implementado en el entorno empresarial de nuestra organización.

La implementación del sistema incluyo:

- Políticas de seguridad baso en la ISO/IE 27001:2013.
- Procedimiento de control de accesos.
- Mejora continua y monitoreo constante

Con la implementación del Sistema de Gestión de Control de Acceso basado en la ISO 27001, CV CONSTRUCCIONES GENERALES S.A.C. busca proteger la seguridad de información. Confirmamos que el sistema está operando según las especificaciones técnicas y cumple con los estándares de calidad y eficiencia requeridos para nuestras operaciones.

Esta certificación se emite a petición de Christian Barrientos Inga para los fines que estime convenientes.

Para constancia de lo anterior, se firma la presente certificación.

Atentamente,

CV CONSTRUCCIONES GENERALES S.A.C

Cesar Vargas Zúñiga
GERENTE GENERAL

Firma del Gerente General

Anexo 9

PreTest

GUIA DE OBSERVACION - PRETEST			
INVESTIGADOR	BARRIENTOS INGA, CHRISTIAN SANTOS		
EMPRESA	Construcciones CV SAC		
DIRECCION	Jr. Chiclayo Nro. 360 Urb. San Felipe - Comas		
DIMENSIÓN	**CONFIDENCIALIDAD**		
MES	AGOSTO	**AÑO**	2023
INDICADOR: Porcentaje total de accesos no autorizados a la información		**FORMULA:** $\text{PTANA} = \frac{\text{ANA}}{\text{AS}} \text{x } 100$	

DIA	Nro. de Accesos al Sistema (AS)	Nro. de Accesos no autorizados (ANA)	Porcentaje total de accesos no autorizados a la información (PTANA)
01/08/2023	20	15	75
02/08/2023	18	14	78
03/08/2023	20	13	65
06/08/2023	19	14	74
07/08/2023	18	10	56
08/08/2023	17	13	76
09/08/2023	20	10	50
10/08/2023	18	15	83
13/08/2023	19	14	74
14/08/2023	20	10	50
15/08/2023	17	14	82
16/08/2023	18	13	72
17/08/2023	19	10	53
20/08/2023	20	10	50
21/08/2023	22	10	45
22/08/2023	17	14	82
23/08/2023	18	14	78
24/08/2023	17	13	76
27/08/2023	17	13	76
28/08/2023	17	14	82
PROMEDIO	**371**	**253**	**68**

GUIA DE OBSERVACION - PRETEST			
INVESTIGADOR	BARRIENTOS INGA, CHRISTIAN SANTOS		
EMPRESA	Construcciones CV SAC		
DIRECCION	Jr. Chiclayo Nro. 360 Urb. San Felipe - Comas		
DIMENSIÓN	**DISPONIBILIDAD**		
MES	AGOSTO	**AÑO**	2023
INDICADOR: **Porcentaje total de inaccesibilidad inmediata a la información**		**FORMULA:** $\text{PTINT} = \frac{\text{SINT}}{\text{SAI}} \text{x } 100$	

DIA	Nro. de Solicitudes de Acceso a la Información (SAI)	Nro. de Solicitudes de acceso a la información interrumpidas (SINT)	Porcentaje total de inaccesibilidad inmediata a la información (PTINT)
01/08/2023	8	6	75
02/08/2023	10	4	40
03/08/2023	9	6	67
06/08/2023	10	5	50
07/08/2023	10	4	40
08/08/2023	9	3	33
09/08/2023	10	4	40
10/08/2023	10	4	40
13/08/2023	8	5	63
14/08/2023	10	4	40
15/08/2023	9	4	44
16/08/2023	10	4	40
17/08/2023	10	4	40
20/08/2023	8	3	38
21/08/2023	10	6	60
22/08/2023	9	4	44
23/08/2023	10	3	30
24/08/2023	8	5	63
27/08/2023	10	4	40
28/08/2023	9	5	56
PROMEDIO	**187**	**87**	**47**

GUIA DE OBSERVACION - PRETEST			
INVESTIGADOR	BARRIENTOS INGA, CHRISTIAN SANTOS		
EMPRESA	Construcciones CV SAC		
DIRECCION	Jr. Chiclayo Nro. 360 Urb. San Felipe - Comas		
DIMENSIÓN	**INTEGRIDAD**		
MES	AGOSTO	**AÑO**	2023
INDICADOR: Porcentaje total de información modificada sin autorización		**FORMULA:** $\text{PTIMA} = \frac{\text{IMA}}{\text{IM}} \text{x } 100$	

DIA	Nro. de Información Modificada (IM)	Nro. de Información Modificada sin Autorización (IMA)	Porcentaje total de información modificada sin autorización (PTIMA)
01/08/2023	22	15	68
02/08/2023	23	10	43
03/08/2023	24	14	58
06/08/2023	22	10	45
07/08/2023	20	10	50
08/08/2023	25	10	40
09/08/2023	20	14	70
10/08/2023	24	15	63
13/08/2023	20	10	50
14/08/2023	22	10	45
15/08/2023	23	10	43
16/08/2023	24	14	58
17/08/2023	20	10	50
20/08/2023	22	10	45
21/08/2023	27	15	56
22/08/2023	25	14	56
23/08/2023	20	10	50
24/08/2023	26	14	54
27/08/2023	22	10	45
28/08/2023	24	15	63
PROMEDIO	**455**	**240**	**53**

Anexo 10

PosTest

GUIA DE OBSERVACION - POSTEST			
INVESTIGADOR	BARRIENTOS INGA, CHRISTIAN SANTOS		
EMPRESA	Construcciones CV SAC		
DIRECCION	Jr. Chiclayo Nro. 360 Urb. San Felipe - Comas		
DIMENSIÓN	**CONFIDENCIALIDAD**		
MES	OCTUBRE	**AÑO**	2023
INDICADOR: Porcentaje total de accesos no autorizados a la información		**FORMULA:** $\text{PTANA} = \frac{\text{ANA}}{\text{AS}} \text{x } 100$	

DIA	Nro. de Accesos al Sistema (AS)	Nro. de Accesos no autorizados (ANA)	Porcentaje total de accesos no autorizados a la información (PTANA)
02/10/2023	15	3	20
03/10/2023	14	4	29
04/10/2023	10	3	30
05/10/2023	15	0	0
06/10/2023	15	3	20
09/10/2023	15	3	20
10/10/2023	15	3	20
11/10/2023	14	2	14
12/10/2023	15	1	7
13/10/2023	15	1	7
16/10/2023	10	0	0
17/10/2023	14	2	14
18/10/2023	15	2	13
19/10/2023	10	1	10
20/10/2023	15	2	13
23/10/2023	15	3	20
24/10/2023	14	3	21
25/10/2023	10	2	20
26/10/2023	15	3	20
27/10/2023	10	1	10
PROMEDIO	**271**	**42**	**15**

GUIA DE OBSERVACION - POSTEST			
INVESTIGADOR	BARRIENTOS INGA, CHRISTIAN SANTOS		
EMPRESA	Construcciones CV SAC		
DIRECCION	Jr. Chiclayo Nro. 360 Urb. San Felipe - Comas		
DIMENSIÓN	**INTEGRIDAD**		
MES	OCTUBRE	**AÑO**	2023
INDICADOR: Porcentaje total de información modificada sin autorización		**FORMULA:** $\text{PTIMA} = \frac{\text{IMA}}{\text{IM}} \text{x } 100$	

DIA	Nro. de Información Modificada (IM)	Nro. de Información Modificada sin Autorización (IMA)	Porcentaje total de información modificada sin autorización (PTIMA)
02/10/2023	22	3	14
03/10/2023	23	5	22
04/10/2023	24	4	17
05/10/2023	22	1	5
06/10/2023	20	0	0
09/10/2023	25	2	8
10/10/2023	20	4	20
11/10/2023	24	2	8
12/10/2023	20	3	15
13/10/2023	22	1	5
16/10/2023	23	5	22
17/10/2023	24	0	0
18/10/2023	20	2	10
19/10/2023	22	2	9
20/10/2023	27	3	11
23/10/2023	25	5	20
24/10/2023	20	3	15
25/10/2023	26	5	19
26/10/2023	22	0	0
27/10/2023	24	2	8
PROMEDIO	**455**	**52**	**11**

GUIA DE OBSERVACION - POSTEST			
INVESTIGADOR	BARRIENTOS INGA, CHRISTIAN SANTOS		
EMPRESA	Construcciones CV SAC		
DIRECCION	Jr. Chiclayo Nro. 360 Urb. San Felipe - Comas		
DIMENSIÓN	**DISPONIBILIDAD**		
MES	OCTUBRE	**AÑO**	2023
INDICADOR: **Porcentaje total de inaccesibilidad inmediata a la información**		**FORMULA:** $\text{PTINT} = \frac{\text{SINT}}{\text{SAI}} \text{x } 100$	

DIA	Nro. de Solicitudes de Acceso a la Información (SAI)	Nro. de Solicitudes de acceso a la información interrumpidas (SINT)	Porcentaje total de inaccesibilidad inmediata a la información (PTINT)
02/10/2023	8	1	13
03/10/2023	9	2	22
04/10/2023	9	1	11
05/10/2023	7	1	14
06/10/2023	9	1	11
09/10/2023	8	0	0
10/10/2023	7	0	0
11/10/2023	8	0	0
12/10/2023	7	0	0
13/10/2023	8	1	13
16/10/2023	8	1	13
17/10/2023	8	1	13
18/10/2023	9	1	11
19/10/2023	7	2	29
20/10/2023	8	0	0
23/10/2023	8	0	0
24/10/2023	7	2	29
25/10/2023	8	2	25
26/10/2023	9	2	22
27/10/2023	8	1	13
PROMEDIO	**160**	**19**	**12**

Anexo 11

Resultado de similitud del programa Turnitin

Turnitin.docx

INFORME DE ORIGINALIDAD

12%	11%	5%	7%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	4%
2	repositorio.ucv.edu.pe Fuente de Internet	2%
3	Submitted to Universidad Abierta para Adultos Trabajo del estudiante	1%
4	www.coursehero.com Fuente de Internet	<1%
5	patents.google.com Fuente de Internet	<1%
6	sceu.frba.utn.edu.ar Fuente de Internet	<1%
7	risti.xyz Fuente de Internet	<1%
8	repositorio.uladech.edu.pe Fuente de Internet	<1%
9	renati.sunedu.gob.pe Fuente de Internet	

Metodología de Producto – ISO/IEC 27001:2013

De acuerdo con los principios establecidos en la norma ISO/IEC 27001:2013, la gestión de la seguridad de la información es fundamental para proteger los activos valiosos de una organización. Uno de los aspectos cruciales en esta gestión es el control de accesos, que se refiere a la capacidad de limitar y supervisar quién tiene permiso para acceder a los recursos y datos sensibles de la empresa.

En el contexto de la norma ISO/IEC 27001:2013, se reconoce la necesidad de implementar un riguroso control de accesos para garantizar la confidencialidad, integridad y disponibilidad de la información. Este control implica establecer políticas y procedimientos claros para autenticar y autorizar a los usuarios, así como para supervisar sus actividades una vez que han obtenido acceso a los sistemas y datos.

La norma ISO/IEC 27001:2013 proporciona directrices detalladas sobre cómo establecer un sistema de control de accesos efectivo. Esto incluye la identificación de usuarios y sus roles, la implementación de autenticación sólida mediante contraseñas seguras, el uso de técnicas de cifrado para proteger los datos durante la transmisión y el establecimiento de políticas de autorización que definen qué recursos específicos pueden ser accedidos por cada usuario.

Además, la norma subraya la importancia de la revisión periódica de los privilegios de acceso, asegurando que los empleados solo tengan acceso a la información necesaria para llevar a cabo sus tareas laborales. Esto no solo reduce el riesgo de accesos no autorizados, sino que también contribuye a una mayor eficiencia operativa al evitar la sobrecarga de información innecesaria para los empleados.

Es esencial mencionar que el control de accesos no se limita solo a los empleados internos, sino que también debe extenderse a terceros, como contratistas y proveedores, que puedan tener acceso a los sistemas y datos de la organización. Establecer políticas y medidas de control robustas para estos usuarios externos es igualmente crucial para mantener la seguridad de la información.

La ISO/IEC 27001:2013 establece directrices claras y específicas para el control de accesos, proporcionando un marco integral para garantizar que las organizaciones protejan adecuadamente sus activos de información, al tiempo que fomentan la eficiencia operativa y la transparencia en el manejo de datos sensibles. Al

implementar estos controles de forma adecuada, las organizaciones pueden fortalecer significativamente su postura de seguridad y mitigar los riesgos asociados con accesos no autorizados.

Metodología de Desarrollo – Ciclo de Deming / PDCA

La implementación de un control de acceso basado en la norma ISO 27001 utilizando el ciclo PDCA (Planificar, Hacer, Verificar, Actuar) es fundamental para garantizar la seguridad de la información en una organización. Aquí se destaca la importancia de este enfoque cíclico en el contexto del control de acceso:

En la fase de "**planificar**", la organización planifica la implementación del control de acceso basándose en los requisitos específicos de la norma ISO 27001. Se establecen políticas claras, se definen roles y responsabilidades, y se desarrollan procedimientos detallados para garantizar un acceso seguro a los recursos de la empresa. La planificación cuidadosa es esencial para anticipar posibles desafíos y asegurar una implementación efectiva del control de acceso.

En la etapa "**hace**", se implementan las políticas y los procedimientos planificados. Se registran usuarios, se establecen niveles de acceso y se configuran sistemas de autenticación. Además, se lleva a cabo la educación y capacitación de los usuarios para garantizar que comprendan las políticas y prácticas seguras relacionadas con el acceso a la información. La fase "Hacer" del ciclo PDCA es crucial para traducir la planificación en acción concreta.

En esta fase de "**verificar**", se realizan revisiones y evaluaciones periódicas del sistema de control de acceso implementado. Se llevan a cabo auditorías internas y revisiones de los derechos de acceso de los usuarios para garantizar que estén alineados con las políticas establecidas y la norma ISO 27001. Esta etapa implica la revisión continua para asegurar que el control de acceso funcione según lo planeado y se ajuste a los requisitos de seguridad.

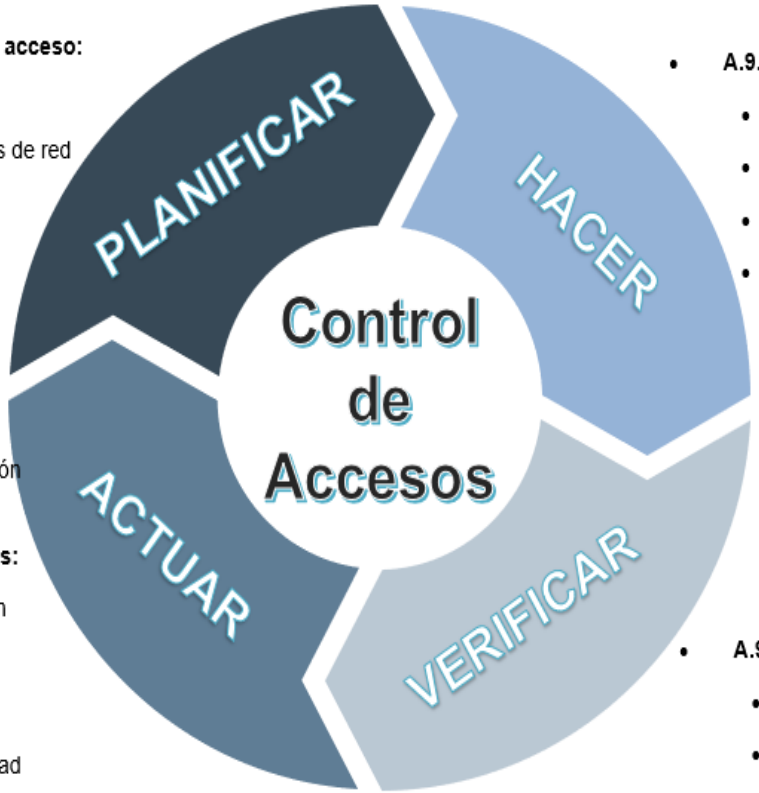
La etapa "**Actuar**" del ciclo PDCA implica tomar medidas basadas en las evaluaciones y revisiones realizadas durante la fase de "Verificar". Si se identifican deficiencias o áreas de mejora en el control de acceso, se toman medidas correctivas. Esto puede incluir ajustes en las políticas, la capacitación adicional de los usuarios o la mejora de los sistemas de autenticación. Además, se consideran

las lecciones aprendidas para mejorar continuamente el sistema de control de acceso de la organización.

La implementación del control de acceso basado en la norma ISO 27001 utilizando el ciclo PDCA garantiza un enfoque sistemático y continuo para mantener la seguridad de la información. Este enfoque cíclico permite a las organizaciones adaptarse a los cambios en el entorno de seguridad, corregir las deficiencias identificadas y mejorar constantemente sus prácticas de control de acceso. Al seguir este proceso iterativo, las organizaciones pueden fortalecer su postura de seguridad y proteger de manera efectiva los activos de información contra amenazas internas y externas.

Plan de implementación del Anexo 9 de la ISO/IEC 27001 con PDCA

- **A.9.1 Requisitos de negocio para el control de acceso:**
  - A.9.1.1 Política de control de acceso
  - A.9.1.2 Acceso a las redes y a los servicios de red



- **A.9.2 Gestión del acceso de usuarios:**
  - A.9.2.1 Registro de usuarios y cancelación del registro
  - A.9.2.2 Gestión de acceso a los usuarios
  - A.9.2.3 Gestión de derechos de acceso privilegiados
  - A.9.2.4 Gestión de la información de autenticación secreta de los usuarios

- **A.9.3 Responsabilidades del usuario:**
  - A.9.3.1 Uso de la información de autenticación secreta
- **A.9.4 Control de acceso a sistemas y aplicaciones:**
  - A.9.4.1 Restricción de acceso a la información
  - A.9.4.2 Procedimientos de conexión seguros
  - A.9.4.3 Sistema de gestión de contraseñas
  - A.9.4.4 Uso de programas de utilidad privilegiados
  - A.9.4.5 Control de acceso al código de programas fuente

- **A.9.2 Gestión del acceso de usuarios (continuación):**
  - A.9.2.5 Revisión de derechos de acceso de usuario
  - A.9.2.6 Remoción o ajuste de los derechos de acceso

ISO/IEC 27001:2013 – A.9.1.1 Política de Control de acceso

1. OBJETIVO

Establecer lineamientos para restringir el acceso a la información y a las instalaciones de procesamiento de información.

Así mismo, asegurar el acceso de usuarios autorizados y evitar el acceso sin autorización alos sistemas y servicios bajo la responsabilidad de CV CONSTRUCCIONES GENERALES S.A.C.

2. ALCANCE

Esta política se aplica a todos los empleados, contratistas y terceros que tienen acceso a los recursos de TI de CV CONSTRUCCIONES GENERALES S.A.C. También se extiende a cualquier recurso de TI utilizado en nombre de la organización, ya sea propiedad de la empresa o de terceros.

3. RESPONSABILIDADES

3.1. Gerentes de CV CONSTRUCCIONES GENERALES

Lo gerente CV CONSTRUCCIONES GENERALES S.A.C. tiene la responsabilidad de:

- Aprobar la política de control de accesos y garantizar su cumplimiento.
- Asignar los recursos necesarios para implementar y mantener los controles de acceso.
- Designar a un responsable de seguridad de la información para supervisar y coordinar las actividades relacionadas con el control de accesos.

3.2. Responsable de Seguridad de la Información

El responsable de seguridad de la información tiene la responsabilidad de:

- Desarrollar, implementar y mantener los controles de acceso basados en los requisitos de la ISO 27001 y las necesidades específicas de CV CONSTRUCCIONES GENERALES S.A.C.
- Coordinar la revisión periódica de los accesos autorizados y las políticas de acceso.
- Proporcionar orientación y capacitación a los empleados sobre las mejores prácticas de control de accesos.

3.3 Empleados y Usuarios Autorizados

Los empleados y usuarios autorizados tienen la responsabilidad de:

- Cumplir con las políticas y procedimientos de control de accesos establecidos por CV CONSTRUCCIONES GENERALES S.A.C.
- Utilizar de manera responsable y segura los recursos de TI.
- Informar cualquier incidente de seguridad o sospecha de acceso no autorizado.

4. POLITICAS

4.1 Identificación y Autenticación

- Se implementarán mecanismos de identificación y autenticación para garantizar que solo

los usuarios autorizados tengan acceso a los recursos de TI.

- Se utilizarán contraseñas robustas y se establecerá una política de cambio regular de contraseñas.
- Se fomentará el uso de la autenticación de múltiples factores para aumentar la seguridad.

4.2 Gestión de Cuentas de Usuario

- Se asignarán privilegios de acceso según los roles y responsabilidades de cada usuario.
- Se revisarán y actualizarán periódicamente los privilegios de acceso para garantizar que sigan siendo apropiados y necesarios.
- Se eliminarán o deshabilitarán las cuentas de usuario inactivas o cuando un empleado deje la organización.

4.3 Control de Acceso Físico

- Se implementarán medidas de seguridad física, como controles de acceso a las instalaciones, para proteger los recursos de TI contra accesos no autorizados.
- Se restringirá el acceso a áreas sensibles o críticas a empleados o terceros que tengan la necesidad de acceso.

4.4 Control de Acceso Lógico

- Se establecerán permisos y restricciones de acceso a los sistemas y aplicaciones en función de los roles y responsabilidades de los usuarios.
- Se implementará un control de acceso basado en el principio de "menos privilegios", otorgando solo los derechos necesarios para realizar las tareas asignadas.

4.5 Monitoreo y Registro de Accesos

- Se implementarán mecanismos de monitoreo y registro de accesos para detectar actividades sospechosas o no autorizadas.
- Se revisarán periódicamente los registros de accesos para identificar posibles incidentes de seguridad y tomar las medidas correctivas correspondientes.

5. Cumplimiento y Revisión

- Se realizarán auditorías internas periódicas para evaluar el cumplimiento de la política de control de accesos y realizar mejoras continuas.
- Se revisarán y actualizarán las políticas y procedimientos de control de accesos según sea necesario, en respuesta a cambios en el entorno operativo o a nuevos riesgos identificados.

Esta política de control de accesos se considera parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) de CV CONSTRUCCIONES GENERALES S.A.C. El incumplimiento de esta política puede resultar en medidas disciplinarias, incluida la terminación del empleo, según las políticas internas de la empresa y las leyes aplicables.

Propuesta de implementación de cámaras de seguridad en la oficina.

Universidad César Vallejo

CV CONSTRUCCIONES GENERALES S.A.C

Propuesta de Implementación de Sistema de Cámaras de Seguridad

Estimado Sr. Cesar Vargas Zúñiga,

Con la presente, me permito dirigirme a usted para proponer la implementación de un sistema integral de cámaras de seguridad en las instalaciones de CV CONSTRUCCIONES GENERALES S.A.C ubicadas en el distrito de Comas. La seguridad de la información y la integridad física de los activos son prioridades que se alinean con los estándares internacionales de la norma ISO 27001:2013, referente a la seguridad de la información.

Contexto y Justificación

La oficina de Comas, albergando el área administrativa y la gerencia general, requiere de un sistema de seguridad robusto que asegure la supervisión y el control de acceso, para mitigar cualquier riesgo potencial que pueda comprometer nuestros valiosos recursos humanos y materiales. La implementación de cámaras de seguridad es un paso crucial para fortalecer nuestras defensas contra incidentes de seguridad y para apoyar la estrategia general de gestión de riesgos de la empresa.

Objetivos de la Implementación

Monitoreo y Registro Continuo: Garantizar la vigilancia constante de los puntos de entrada y áreas críticas de nuestras instalaciones.

Referente de Actividades no Autorizadas: Desalentar y detectar intrusiones, robos o cualquier otra actividad irregular.

Cumplimiento de Normativas: Cumplir con la cláusula A.9.1.1 de la norma ISO 27001:2013, que trata sobre el control de acceso físico.

Solución Propuesta

La solución consistirá en la instalación de cámaras de seguridad de alta definición con capacidad de grabación nocturna y almacenamiento seguro de datos. Estas cámaras estarán conectadas a una central de monitoreo operada por personal calificado, asegurando una respuesta rápida ante cualquier evento.

Impacto y Beneficios

Prevención de Riesgos: Reducción significativa de la probabilidad de incidentes de seguridad.

Respuesta a Incidentes: Capacidad mejorada para responder y gestionar incidentes de seguridad de manera efectiva.

Conformidad y Confianza: Refuerzo de la confianza de los stakeholders en la gestión de la seguridad de la empresa.

Costos y Consideraciones

Se realizará un análisis detallado de costos y se presentará un presupuesto detallado tras la evaluación preliminar de las instalaciones. Se considerarán opciones de financiamiento y se buscarán alternativas que maximicen la relación costo-beneficio.

Siguientes Pasos

Solicito la oportunidad de discutir esta propuesta en una reunión para detallar el alcance y las especificaciones técnicas del sistema de cámaras de seguridad propuesto. Espero poder colaborar con CV CONSTRUCCIONES GENERALES S.A.C en la implementación de esta importante mejora en la seguridad.

Agradezco de antemano su atención y quedo a la espera de su respuesta para coordinar una fecha y hora convenientes para usted.

Atentamente,

Christian Barrientos Inga

Estudiante de Ingeniería de Sistemas

Anexo: Este cuadro es una simulación y los costos son estimados basados en precios promedio del mercado en Perú. Los precios reales pueden variar y es recomendable solicitar cotizaciones.

Concepto	**Marca**	**Costo Unitario (PEN)**	**Cantidad**	**Costo Total (PEN)**
Cámaras de seguridad Full HD	HIKVISION	200	4	800
DVR/NVR con almacenamiento de 1 TB	DAHUA	500	1	500
Cableado y accesorios de instalación	GENÉRICO	100	1	100
Instalación y configuración por cámara	SERVICIO LOCAL	150	4	600
Capacitación para el uso del sistema	SERVICIO LOCAL	200	1	200
Total, Estimado sin IGV				**2200**

Nota: Este cuadro es una simulación y los costos son estimados basados en precios promedio del mercado en Perú. Los precios reales pueden variar y es recomendable solicitar cotizaciones.

ISO/IEC 27001:2013 – A.9.1.2 Acceso a las redes y a los servicios de las redes

1. INTRODUCCION

La política de acceso a redes y servicios establece los lineamientos y procedimientos para garantizar la seguridad y el acceso adecuado a las redes y los servicios de tecnología de la información (TI) en CV CONSTRUCCIONES GENERALES S.A.C. El objetivo de esta política es proteger la confidencialidad, integridad y disponibilidad de la información y los sistemas de información de la organización.

2. ALCANCE

Esta política se aplica a todos los empleados, contratistas y terceros que tienen acceso a los recursos de TI de CV CONSTRUCCIONES GENERALES S.A.C. También se extiende a cualquier dispositivo, infraestructura de red y servicio utilizado en nombre de la organización, ya sea propiedad de la empresa o de terceros. terceros.

3. RESPONSABILIDADES

3.1. Alta Dirección

La alta dirección de CV CONSTRUCCIONES GENERALES S.A.C. tiene la responsabilidad de:

- Aprobar la política de acceso a redes y servicios y garantizar su cumplimiento.
- Asignar los recursos necesarios para implementar y mantener los controles de acceso.
- Designar a un responsable de seguridad de la información para supervisar y coordinar las actividades relacionadas con el acceso a redes y servicios.

3.2. Responsable de Seguridad de la Información

El responsable de seguridad de la información tiene la responsabilidad de:

- Desarrollar, implementar y mantener los controles de acceso a redes y servicios basados en los requisitos de la ISO 27001 y las necesidades específicas de CV CONSTRUCCIONES GENERALES S.A.C.
- Coordinar la revisión periódica de los accesos autorizados y las políticas de acceso a redes y servicios.
- Proporcionar orientación y capacitación a los empleados sobre las mejores prácticas de acceso a redes y servicios.

3.3 Empleados y Usuarios Autorizados

Los empleados y usuarios autorizados tienen la responsabilidad de:

- Cumplir con las políticas y procedimientos de acceso a redes y servicios establecidos por CV CONSTRUCCIONES GENERALES S.A.C.

- Utilizar de manera responsable y segura las redes y servicios de TI.
- Informar cualquier incidente de seguridad o sospecha de acceso no autorizado a redes y servicios.

4. POLITICAS DE ACCESO A REDES Y SERVICIOS

4.1 Segmentación de Redes

- Se implementará una segmentación de redes para separar los sistemas y servicios según su nivel de confidencialidad y criticidad.
- Se establecerán firewalls y otras medidas de seguridad para controlar y filtrar el tráfico entre las diferentes redes.

4.2 Autenticación y Autorización

- Se implementarán mecanismos de autenticación y autorización para garantizar que solo los usuarios autorizados tengan acceso a las redes y servicios.
- Se utilizarán contraseñas robustas y se establecerá una política de cambio regular de contraseñas.

4.3 Gestión de Permisos de Acceso

- Se asignarán permisos y privilegios de acceso a los usuarios según sus roles y responsabilidades.
- Se revisarán y actualizarán periódicamente los permisos de acceso para garantizar que sigan siendo apropiados y necesarios.
- Se eliminarán o deshabilitarán los permisos de acceso cuando un empleado cambie de rol o deje la organización.

4.4 Monitoreo de Redes y Servicios

- Se implementarán herramientas de monitoreo de redes y servicios para detectar y responder a eventos de seguridad.
- Se revisarán periódicamente los registros de actividad de las redes y servicios para identificar posibles incidentes de seguridad y tomar las medidas correctivas correspondientes.

4.5 General

– Todas las solicitudes para conectar equipos de cómputo a la red de la organización deberán ser revisadas por el responsable del área o proceso involucrado y el Administrador

de Redes y Comunicaciones, para garantizar que se cumplan los requisitos de seguridad establecidos.

– Todos los accesos a los servicios informáticos, deberán basarse en el Principio de Menor Acceso (permiso nulo por defecto), de acuerdo con los requerimientos.

– Todos los cambios de acceso a la red deben ir acompañados de una justificación válida relacionada y ceñida al análisis de seguridad. Si existe un incidente de seguridad o se identifica que existe un acceso a la red de forma indebida, se modifica los permisos actuales, o en su defecto, se pone fin a la conexión.

5. CUMPLIMIENTO Y REVISIÓN

- Se realizarán auditorías internas periódicas para evaluar el cumplimiento de la política de control de accesos y realizar mejoras continuas.
- Se revisarán y actualizarán las políticas y procedimientos de control de accesos según sea necesario, en respuesta a cambios en el entorno operativo o a nuevos riesgos identificados.

Esta política de acceso a redes y servicios se considera parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) de CV CONSTRUCCIONES GENERALES S.A.C. El incumplimiento de esta política puede resultar en medidas disciplinarias, incluida la terminación del empleo, según las políticas internas de la empresa y las leyes aplicables.

ISO/IEC 27001:2013 – A.9.2.1 Registro y baja de usuario

1. OBJETIVO

El objetivo de este proceso es establecer un procedimiento formal para el registro y cancelación de usuarios en los sistemas y servicios de tecnología de la información (TI) en CV CONSTRUCCIONES GENERALES S.A.C. Este proceso garantizará que los usuarios autorizados tengan los derechos de acceso adecuados y que se tomen las medidas necesarias al dar de baja a los usuarios que ya no requieren acceso.

2. ALCANCE

Este proceso se aplica a todos los empleados, contratistas y terceros que requieren acceso a los sistemas y servicios de TI de CV CONSTRUCCIONES GENERALES S.A.C. También se extiende a cualquier recurso de TI utilizado en nombre de la organización, ya sea propiedad de la empresa o de terceros.

3. RESPONSABILIDADES

3.1. Responsable de Seguridad de la Información

El responsable de seguridad de la información tiene la responsabilidad de:

- Coordinar y supervisar el proceso de registro y cancelación de usuarios.
- Establecer y mantener un formulario o sistema de solicitud de acceso y baja de usuarios.
- Verificar la documentación y la aprobación necesarias para el registro y cancelación de usuarios.

3.2. Departamento de Recursos Humanos

El departamento de recursos humanos tiene la responsabilidad de:

- Notificar al responsable de seguridad de la información sobre los empleados nuevos o los cambios de estado de los empleados existentes, como cambios de roles o desvinculaciones.

3.3. Jefes y Supervisores

Los jefes y supervisores tienen la responsabilidad de:

- Proporcionar la aprobación y la justificación para el acceso de los empleados bajo su supervisión.
- Notificar al responsable de seguridad de la información sobre los cambios de roles o desvinculaciones de los empleados bajo su supervisión.

4. PROCESO DE REGISTRO DE USUARIOS

4.1. Inicio:

- El usuario inicia el proceso enviando una solicitud de alta o modificando una solicitud previa si es necesario.

4.2. Recepción y Análisis de la Solicitud:

- El equipo de soporte de TI recibe y revisa la solicitud para asegurar que contiene toda la información necesaria.
- Se analiza el caso y se actualiza su estado en el sistema de seguimiento.

4.3. Validación de Requisitos:

- Si la solicitud no cumple con los criterios establecidos, se envía un correo al usuario solicitando las modificaciones pertinentes.
- Si cumple con los requisitos, se envía un correo de aprobación al usuario y se actualiza el estado del caso.

4.4. Aprobación de la Solicitud:

- La solicitud de caso es aprobada por la jefatura y el soporte correspondiente.
- Se recibe y valida la aprobación.

4.5. Actualización en Active Directory:

- Se actualiza la información del usuario en el sistema (AD)
- Se crea el usuario con el perfil necesario

4.6. Provisión de Accesos:

- Se configuran los accesos para el usuario, lo que puede incluir la creación de una cuenta de usuario de dominio y acceso a VPN.
- Se valida que la solución cumpla con los requisitos del ticket.

4.7. Finalización y Confirmación:

- Se envía al usuario la información de alta junto con las credenciales y detalles de acceso.
- El usuario confirma que ha recibido el acceso y que todo funciona correctamente.
- Se actualiza el estado del caso para reflejar que la solicitud de alta ha sido completada y cerrada.

4.8. Fin del Proceso:

El proceso termina con la validación del alta y la conformidad del usuario con el acceso proporcionado.

5. PROCESO DE CANCELACIÓN DE USUARIOS

5.1 Notificación de Cambios de Estado

- El departamento de recursos humanos notificará al responsable de seguridad de la información sobre cualquier cambio de estado de los empleados, como cambios de roles o desvinculaciones.

5.2 Desactivación de Cuentas y Revocación de Derechos

- El responsable de seguridad de la información desactivará la cuenta de usuario en los sistemas y servicios correspondientes y revocará todos los derechos de acceso del usuario.
- Se revisarán y actualizarán los registros de acceso para reflejar la cancelación del usuario.

6. REVISIÓN Y MEJORA CONTINUA

- Se realizarán revisiones periódicas del proceso de registro y cancelación de usuarios para identificar áreas de mejora y tomar las acciones correctivas correspondientes.
- Se actualizará la documentación y los formularios de solicitud según sea necesario para reflejar los cambios y requisitos actuales.

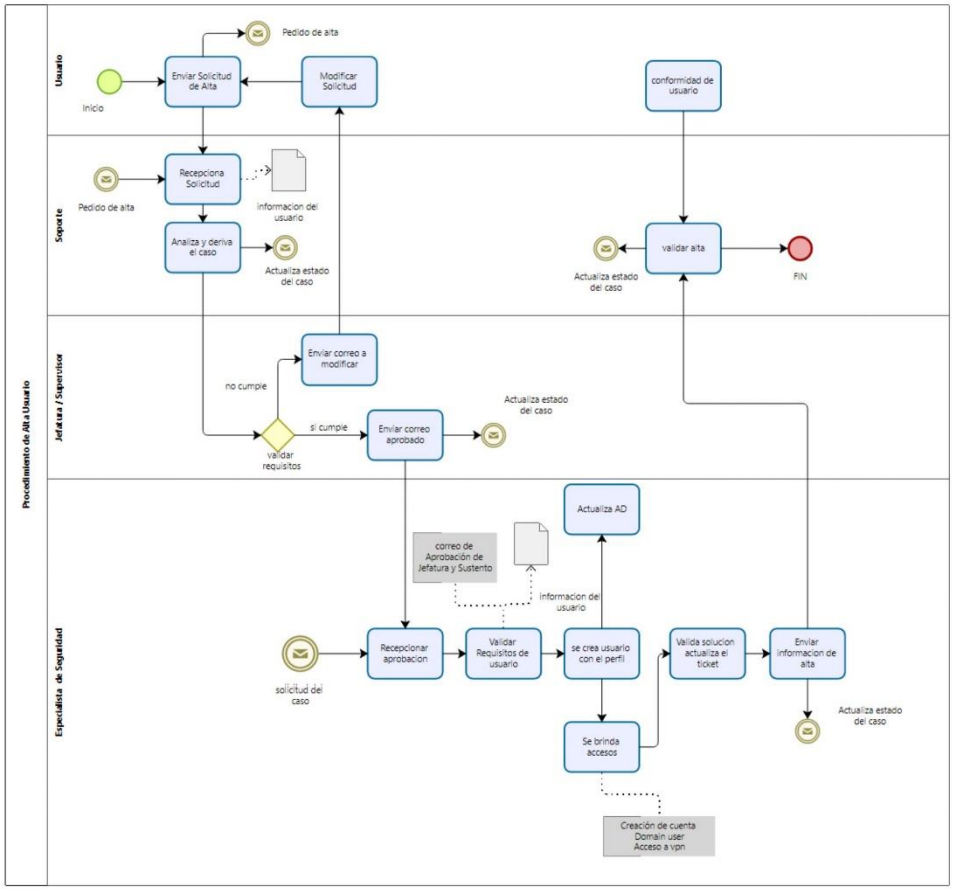
Este proceso de registro y cancelación de usuarios se considera parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) de CV CONSTRUCCIONES GENERALES S.A.C. El incumplimiento de esta política puede resultar en medidas disciplinarias, incluida la terminación del empleo, según las políticas internas de la empresa y las leyes aplicables.

Procedimiento de Alta al Colaborador

Universidad César Vallejo

CV CONSTRUCCIONES GENERALES S.A.C

Flujo de Alta de Usuario



ISO/IEC 27001:2013 – A.9.2.2 Provisión de acceso al usuario

1. OBJETIVO

El objetivo de este proceso es establecer un procedimiento formal para el aprovisionamiento de acceso de usuarios a los sistemas, file, documentos, archivos y servicios de tecnología de la información (TI) de CV CONSTRUCCIONES GENERALES S.A.C. Este proceso garantizará que los usuarios autorizados obtengan los derechos de acceso adecuados de manera oportuna y segura.

2. ALCANCE

Este proceso se aplica a todos los empleados, contratistas y terceros que requieren acceso a los sistemas y servicios de TI de CV CONSTRUCCIONES GENERALES S.A.C. También se extiende a cualquier recurso de TI utilizado en nombre de la organización, ya sea propiedad de la empresa o de terceros.

3. RESPONSABILIDADES

3.1. Responsable de Seguridad de la Información

El responsable de seguridad de la información tiene la responsabilidad de:

- Coordinar y supervisar el proceso de aprovisionamiento de acceso de usuarios.
- Establecer y mantener un formulario o sistema de solicitud de aprovisionamiento de acceso de usuarios.
- Verificar la documentación y la aprobación necesarias para el aprovisionamiento de acceso.

3.2. Jefes y Supervisores

Los jefes y supervisores tienen la responsabilidad de:

- Identificar y justificar los derechos de acceso requeridos para los empleados bajo su supervisión.

Proporcionar la aprobación para el aprovisionamiento de acceso de los empleados bajo su supervisión.

4. PROCESO DE APROVISIONAMIENTO DE ACCESO DE USUARIOS

4.1. Inicio:

- El usuario solicita acceso o permisos para un archivo o documento dentro del repositorio.

4.2. Recepción de la Solicitud:

- Soporte de TI recibe la solicitud y revisa la información del usuario proporcionada.

4.3. Análisis y Derivación del Caso:

- Soporte de TI analiza la solicitud y actualiza el estado del caso en el sistema de seguimiento.
- Si la solicitud no cumple con los criterios, se solicita al usuario que modifique su solicitud.
- Si la solicitud cumple, se envía un correo de aprobación y se actualiza el estado del caso.

4.4. Aprobación:

- Jefatura y Soporte reciben y revisan la solicitud de caso.
- Se valida que los requisitos del usuario estén acordes con las políticas de acceso.
- Si es aprobada, Soporte de TI procede con la configuración de permisos.

4.5. Configuración de Acceso:

- Se modifica el perfil del usuario según las especificaciones aprobadas.
- Se crea un grupo de seguridad en Active Directory y se asocia al repositorio.

4.6. Validación y Confirmación:

- Se valida la solución y se actualiza el ticket de seguimiento.
- Se envía al usuario la información de los permisos concedidos.
- El usuario confirma la conformidad con los accesos recibidos.

4.7. Fin del Proceso:

El proceso termina con la validación del acceso al repositorio y la conformidad del usuario.

5. REVISION Y ACTUALIZACION DE DERECHOS DE ACCESO

El responsable de seguridad de la información revisará periódicamente los derechos de acceso asignados a los usuarios para garantizar que sigan siendo apropiados y necesarios.

Se realizarán ajustes en los derechos de acceso en caso de cambios de roles, traslados o cambios en las responsabilidades de los empleados.

6. REVISIÓN Y MEJORA CONTINUA

Se realizarán revisiones periódicas del proceso de aprovisionamiento de acceso de usuarios para identificar áreas de mejora y tomar las acciones correctivas correspondientes.
Se actualizará la documentación y los formularios de solicitud según sea necesario para reflejar los cambios y requisitos actuales.

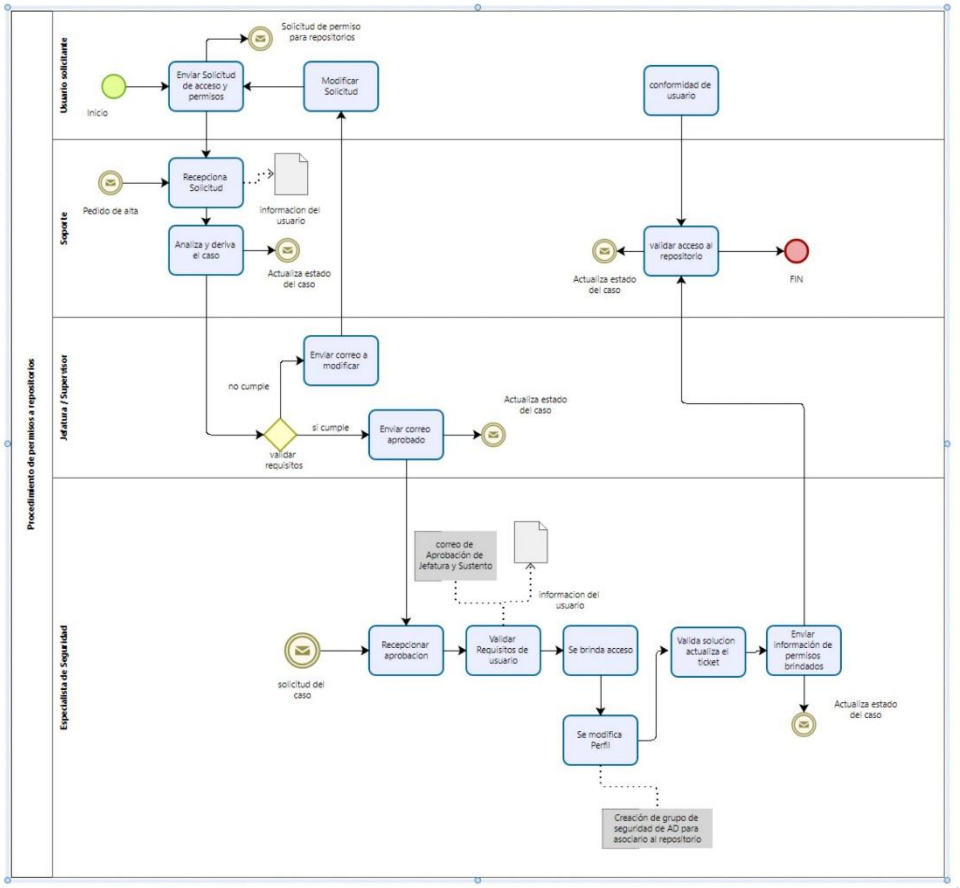
Este proceso de aprovisionamiento de acceso de usuarios se considera parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) de CV CONSTRUCCIONES GENERALES S.A.C. El incumplimiento de este proceso puede resultar en medidas disciplinarias, según las políticas internas de la empresa y las leyes aplicables.

Procedimiento de permiso a repositorio

Universidad César Vallejo

CV CONSTRUCCIONES GENERALES S.A.C

Flujo de Permisos a Repositorios



ISO/IEC 27001:2013 – A.9.2.3 Gestión de derecho de acceso privilegiado

1. OBJETIVO

El objetivo de este proceso es establecer un procedimiento formal para la gestión de los derechos de acceso privilegiado en los sistemas y servicios de tecnología de la información (TI) de CV CONSTRUCCIONES GENERALES S.A.C. Este proceso garantizará que los derechos de acceso privilegiado sean otorgados de manera segura, controlada y supervisada para minimizar los riesgos asociados.

2. ALCANCE

Este proceso se aplica a todos los empleados, contratistas y terceros que tienen derechos de acceso privilegiado a los sistemas y servicios de TI de CV CONSTRUCCIONES GENERALES S.A.C. También se extiende a cualquier recurso de TI utilizado en nombre de la organización, ya sea propiedad de la empresa o de terceros.

3. RESPONSABILIDADES

3.1. Responsable de Seguridad de la Información

El responsable de seguridad de la información tiene la responsabilidad de:

- Coordinar y supervisar el proceso de gestión de derechos de acceso privilegiado.
- Establecer y mantener un registro centralizado de los usuarios con derechos de acceso privilegiado.
- Verificar la documentación y la aprobación necesarias para otorgar o modificar los derechos de acceso privilegiado.

3.2 Usuarios con Derechos de Acceso Privilegiado

Los usuarios con derechos de acceso privilegiado tienen la responsabilidad de:

- Utilizar sus derechos de acceso privilegiado de manera adecuada y solo para los fines autorizados.
- Cumplir con las políticas y procedimientos establecidos para el uso de los derechos de acceso privilegiado.
- Informar cualquier actividad sospechosa o incidente relacionado con los derechos de acceso privilegiado al responsable de seguridad de la información.

4. PROCESO DE GESTION DE DERECHOS DE ACCESO PRIVILEGIADO

4.1 Identificación de Usuarios con Derechos de Acceso Privilegiado

El responsable de seguridad de la información identificará los usuarios que requieren derechos de acceso privilegiado en función de las necesidades del negocio y los roles asignados.

4.2 Verificación de Antecedentes y Aprobación

Antes de otorgar derechos de acceso privilegiado, se realizará una verificación de antecedentes apropiada para los usuarios identificados.

El responsable de seguridad de la información obtendrá la aprobación final de los gerentes o supervisores correspondientes antes de otorgar los derechos de acceso privilegiado.

4.3 Otorgamiento de Derechos de Acceso Privilegiado

El responsable de seguridad de la información creará las cuentas de usuario con derechos de acceso privilegiado en los sistemas y servicios correspondientes.

Los derechos de acceso privilegiado se asignarán de manera específica y restringida según las responsabilidades y funciones del usuario.

4.4 Monitoreo y Auditoría

Se implementarán mecanismos de monitoreo y auditoría para registrar las actividades realizadas por los usuarios con derechos de acceso privilegiado.

Se revisarán regularmente los registros de actividades para detectar y responder a cualquier actividad sospechosa o inapropiada.

5. REVISION Y ACTUALIZACION DE DERECHOS DE ACCESO PRIVILEGIADO

El responsable de seguridad de la información realizará revisiones periódicas de los derechos de acceso privilegiado para garantizar que sigan siendo necesarios y justificados.

Se realizarán ajustes en los derechos de acceso privilegiado en caso de cambios en los roles o responsabilidades de los usuarios.

6. REVISIÓN Y MEJORA CONTINUA

Se realizarán revisiones periódicas del proceso de gestión de derechos de acceso privilegiado para identificar áreas de mejora y tomar las acciones correctivas correspondientes.

Se actualizará la documentación y los registros según sea necesario para reflejar los cambios y requisitos actuales.

Este proceso de gestión de derechos de acceso privilegiado se considera parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) de CV CONSTRUCCIONES GENERALES S.A.C. El incumplimiento de este proceso puede resultar en medidas disciplinarias, según las políticas internas de la empresa y las leyes aplicables.

Informe de pretest sobre accesos privilegiado para usuarios del dominio

Universidad César Vallejo

A.9.2.3 GESTIÓN DE DERECHO DE ACCESO PRIVILEGIADO

INFORME DE AUDITORIA

Septiembre 2023

BASE DE USUARIOS DE LA EMPRESA

Cliente: CV CONSTRUCCIONES GENERALES S.A.C.

CV CONSTRUCCIONES GENERALES S.A.C

Realizado: Christian Barrientos Inga

TABLA DE CONTENIDO

OBJETIVO

ALCANCE

PERMISOS CARPETA DE RED

OBJETIVO

El objetivo del presente documento es informar y detallar sobre los permisos de accesos privilegiados que se tiene en el dominio de CV CONSTRUCCIONES GENERALES SAC

ALCANCE

Documento aplicable al área Seguridad de la Información de la empresa CV CONSTRUCCIONES GENERALES S.A.C.

RESUMEN

La presente información detalla los permisos dentro del dominio local de la empresa CV CONSTRUCCIONES GENERALES S.A.C donde se evidenciará en el reporte para un control de acceso.

PERMISOS EN CARPETA DE RED

1. Ruta del dominio

El dominio de la empresa CV CONSTRUCCIONES GENERALES S.A.C esta ubicado en la OU: peru.local que administra una base de datos de aproximadamente 50 usuarios (proveedores y colaboradores).

2. Tipo de permisos privilegiado

Dentro del dominio se evidenciaron 3 permisos privilegiados:

Enterprise Admins: Tienen control total sobre todos los dominios dentro de un bosque de AD. Son útiles en ambientes con múltiples dominios o configuraciones de dominio padre-hijo.

Domain Admins: Presentes en cada dominio, tienen control total sobre su dominio específico, incluyendo todos los servidores y estaciones de trabajo unidos al dominio, y el propio Active Directory.

Administrators: Tienen privilegios administrativos a nivel de sistema local y pueden tener diferentes niveles de privilegios en el dominio si incluyen a Administradores de Dominio como miembros.

3. Usuario con Accesos y tipo de permiso

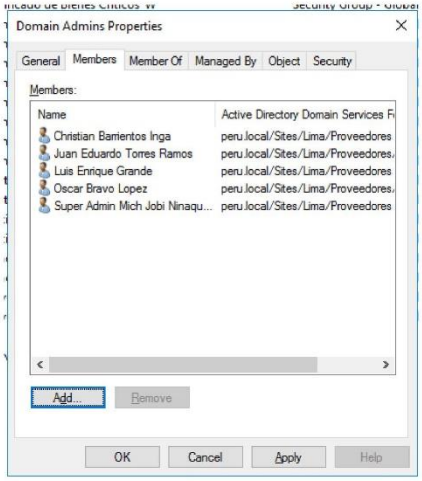
SamAccount	Name	Descripción	Group	Enabled	Tipo
s_mninaquispe	Super Admin Mich Jobi Ninaquispe Angulo	Usuario de Soporte	Domain Admins	True	Usuario
S_OBravo	Oscar Bravo Lopez	Usuario de Soporte	Domain Admins	True	Usuario
s_lgrande	Luis Enrique Grande	Usuario de Soporte	Domain Admins	True	Usuario
s_jtorres	Juan Eduardo Torres Ramos	Usuario de Soporte	Domain Admins	True	Usuario
s_cbarrientos	Christian Barrientos Inga	Usuario de Seguridad de Información	Domain Admins	True	Usuario
usr_citrix_prd	Usuario Citrix PRD	Usuario de servicio Citrix PRD	Enterprise Admins	True	Usuario

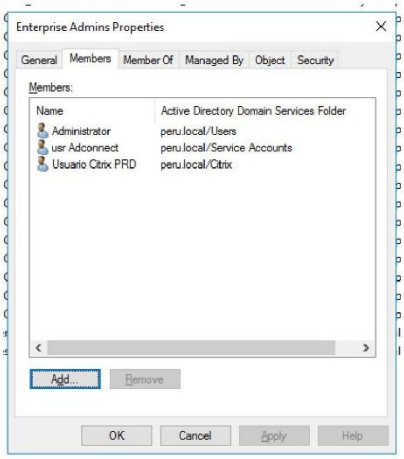
usr_adconnect	usr Adconnect	Usuario para instalación de servicio ADCONNECT	Enterprise Admins	True	Usuario
Administrator	Administrator	Administrador	Enterprise Admins	True	Usuario
Administrator	Administrator	Administrador	Administrators	True	Usuario
Domain Admins	Domain Admins	Grupo de seguridad	Administrators	True	Grupo
Enterprise Admins	Enterprise Admins	Grupo de seguridad	Administrators	True	Grupo

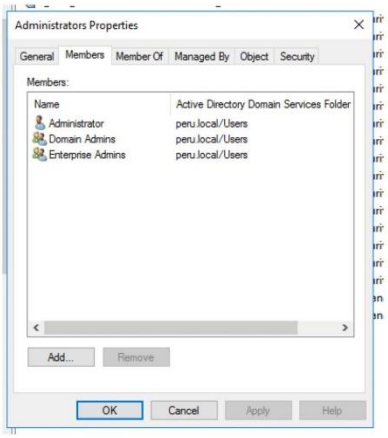
4. Recomendaciones

Se aconseja no emplear el grupo de Administradores de Empresa (Enterprise Admins), puesto que su uso no resulta práctico al gestionar múltiples dominios. Es más efectivo mantener a los usuarios con privilegios concentrados en un único grupo para que el acceso de alto nivel esté más regulado. Además, se sugiere remover a los usuarios de soporte técnico del grupo de Administradores de Dominio (Domain Admins), ya que no necesitan derechos elevados en el dominio de la empresa para desempeñar sus tareas técnicas. Estos usuarios deberían ser reasignados al grupo de Administradores (Administrators) para que puedan realizar sus funciones con los usuarios finales de manera adecuada.

5. Evidencia




Enterprise Admins Properties
General
Members
Member Of
Managed By
Object
Security
Members:
Name
Active Directory Domain Services Folder
Administrator
peru.local/Users
usr Adconnect
peru.local/Service Accounts
Usuario Citrix PRD
peru.local/Citrix
Add...
Remove
OK
Cancel
Apply
Help


Administrators Properties
General
Members
Member Of
Managed By
Object
Security
Members:
Name
Active Directory Domain Services Folder
Administrator
peru.local/Users
Domain Admins
peru.local/Users
Enterprise Admins
peru.local/Users
Add...
Remove
OK
Cancel
Apply
Help

Informe de postest sobre accesos privilegiado para usuarios del dominio

Universidad César Vallejo

A.9.2.3 GESTIÓN DE DERECHO DE ACCESO PRIVILEGIADO

INFORME DE AUDITORIA

Octubre 2023

BASE DE USUARIOS DE LA EMPRESA

Cliente: CV CONSTRUCCIONES GENERALES S.A.C.

CV CONSTRUCCIONES GENERALES S.A.C

Realizado: Christian Barrientos Inga

TABLA DE CONTENIDO

OBJETIVO

ALCANCE

PERMISOS CARPETA DE RED

OBJETIVO

El objetivo del presente documento es informar y detallar sobre los permisos de accesos privilegiados que se tiene en el dominio de CV CONSTRUCCIONES GENERALES SAC

ALCANCE

Documento aplicable al área Seguridad de la Información de la empresa CV CONSTRUCCIONES GENERALES S.A.C.

RESUMEN

La presente información detalla los permisos dentro del dominio local de la empresa CV CONSTRUCCIONES GENERALES S.A.C donde se evidenciará en el reporte para un control de acceso.

PERMISOS EN CARPETA DE RED

1. Ruta del dominio

El dominio de la empresa CV CONSTRUCCIONES GENERALES S.A.C está ubicado en la OU: peru.local que administra una base de datos de aproximadamente 50 usuarios (proveedores y colaboradores).

2. Tipo de permisos privilegiado

Dentro del dominio se evidenciaron 3 permisos privilegiados:

Enterprise Admins: Tienen control total sobre todos los dominios dentro de un bosque de AD. Son útiles en ambientes con múltiples dominios o configuraciones de dominio padre-hijo.

Domain Admins: Presentes en cada dominio, tienen control total sobre su dominio específico, incluyendo todos los servidores y estaciones de trabajo unidos al dominio, y el propio Active Directory.

Administrators: Tienen privilegios administrativos a nivel de sistema local y pueden tener diferentes niveles de privilegios en el dominio si incluyen a Administradores de Dominio como miembros.

3. Usuario con Accesos y tipo de permiso

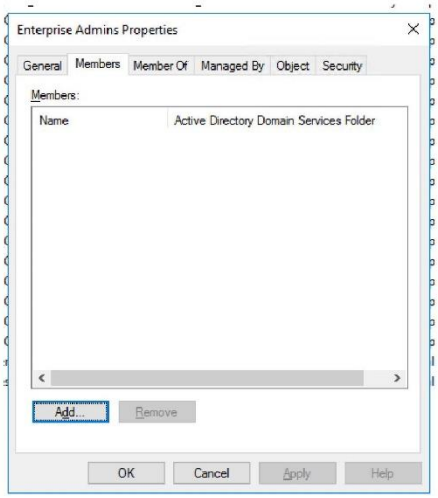
SamAccount	Name	Descripción	Group	Enabled	Tipo
s_lgrande	Luis Enrique Grande	Usuario de Soporte	Administrators	True	Usuario
s_jtorres	Juan Eduardo Torres Ramos	Usuario de Soporte	Administrators	True	Usuario
Administrator	Administrator	Administrador	Administrators	True	Usuario
Domain Admins	Domain Admins	Grupo de seguridad	Administrators	True	Grupo
Enterprise Admins	Enterprise Admins	Grupo de seguridad	Administrators	True	Grupo

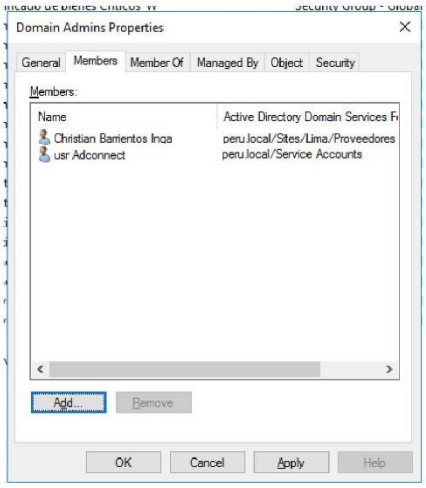
s_cbarrientos	Christian Barrientos Inga	Usuario de Seguridad de Informacipon	Domain Admins	True	Usuario
usr_adconnect	usr Adconnect	Usuario para instalación de servicio ADCONNECT	Domain Admins	True	Usuario

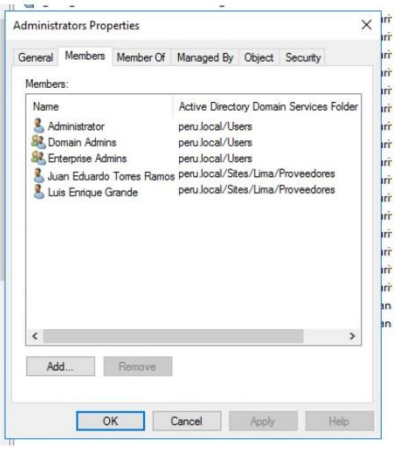
4. Recomendaciones

Se aconseja realizar un monitoreo de las cuentas, debido a sus privilegios sobre equipos y usuario del dominio de la organización, lo cual debe validar constantemente.

5. Evidencia




Domain Admins Properties
General
Members
Member Of
Managed By
Object
Security
Members:
Name
Active Directory Domain Services Fo
Christian Barrientos Inga
peru.local/Sites/Lima/Proveedores
usr Adconnect
peru.local/Service Accounts
Add...
Remove
OK
Cancel
Apply
Help


Administrators Properties
General
Members
Member Of
Managed By
Object
Security
Members:
Name
Active Directory Domain Services Folder
Administrator
peru.local/Users
Domain Admins
peru.local/Users
Enterprise Admins
peru.local/Users
Juan Eduardo Torres Ramos
peru.local/Sites/Lima/Proveedores
Luis Enrique Grande
peru.local/Sites/Lima/Proveedores
Add...
Remove
OK
Cancel
Apply
Help

Script desarrollado en PowerShell para el reporte de Usuario

CV CONSTRUCCIONES GENERALES S.A.C

Universidad César Vallejo

Script (PowerShell para auditoria de Acceso privilegiado)

```
# Importar el módulo de Active Directory
Import-Module ActiveDirectory
# Definir la ruta de salida del archivo CSV
$csvPath = "C:\Users\s_cbarrientos\Desktop\ReporteGeneral.csv"

# Definir los grupos de interés
$groups = @("Enterprise Admins", "Domain Admins", "Administrators")

# Función para obtener el tipo de usuario según el grupo
function Get-UserType {
  param ($user)
  foreach ($group in $groups) {
    $groupMembers = Get-ADGroupMember -Identity $group -Recursive | Select -
ExpandProperty SamAccountName
    if ($groupMembers -contains $user.SamAccountName) {
      return $group
    }
  }
  return $null
}

# Recorrer los grupos y recopilar información de usuarios
$results = foreach ($group in $groups) {
  # Obtener los usuarios del grupo actual con los atributos adicionales
  $users = Get-ADGroupMember -Identity $group -Recursive | Get-ADUser -Properties
DisplayName, SamAccountName, WhenCreated, City, Department, Enabled, CanonicalName,
LastLogon, PasswordLastSet, AccountExpirationDate, PasswordExpired, PasswordNeverExpires,
LastLogonDate, "msDS-UserPasswordExpiryTimeComputed", DistinguishedName, PostalCode,
EmailAddress, OfficePhone, Manager
```

```
    # Recorrer los usuarios y extraer los datos necesarios
    foreach ($user in $users) {
        $userType = Get-UserType -user $user
        $managerDetails = if ($user.Manager) { Get-ADUser -Identity $user.Manager -Properties
DisplayName } else { $null }
        $managerName = $managerDetails.DisplayName
        [PSCustomObject]@{
            "NOMBRE COMPLETO" = $user.DisplayName
            "USUARIO DE RED" = $user.SamAccountName
            "SUBGERENCIA" = $user.City
            "DIRECCIÓN" = $user.Department
            "CÓDIGO POSTAL" = $user.PostalCode
            "E-MAIL" = $user.EmailAddress
            "TELÉFONO" = $user.OfficePhone
            "GERENTE" = $managerName
            "TIPO" = $userType
            "ESTADO" = if ($user.Enabled) { "Enabled" } else { "Disabled" }
            "F. CREACIÓN" = $user.WhenCreated
            "ULT. MODIFICACIÓN" = $user.LastLogonDate
            "ULT. INICIO DE SESIÓN" = if ($user.LastLogon -ne $null) {
[DateTime]::FromFileTime($user.LastLogon) } else { $null }
            "ULT. MODF. CONTRASEÑA" = $user.PasswordLastSet
            "F. EXPI. DE CONTRASEÑA" = if ($user.PasswordNeverExpires) { "Password never expires" }
else { [datetime]::FromFileTime($user."msDS-UserPasswordExpiryTimeComputed").ToString("yyyy-
MM-dd HH:mm:ss") }
            "CADUCIDA DE CUENTA" = $user.AccountExpirationDate
        }
    }
}

# Exportar los resultados al archivo CSV con formato UTF-8
$results | Export-Csv -Path $csvPath -NoTypeInformation -Encoding UTF8
```

ISO/IEC 27001:2013 – A.9.2.4 Gestión de la información de autenticación secreta de los usuarios

1. OBJETIVO

El objetivo de este proceso es establecer un procedimiento formal para la gestión de la información secreta de autenticación de los usuarios en los sistemas y servicios de tecnología de la información (TI) de CV CONSTRUCCIONES GENERALES S.A.C. Este proceso garantizará la protección adecuada de la información secreta utilizada para autenticar a los usuarios, como contraseñas y claves, con el fin de prevenir el acceso no autorizado y los posibles incidentes de seguridad.

2. ALCANCE

Este proceso se aplica a todos los empleados, contratistas y terceros que utilizan sistemas y servicios de TI de CV CONSTRUCCIONES GENERALES S.A.C. y requieren información secreta de autenticación para acceder a ellos. También se extiende a cualquier recurso de TI utilizado en nombre de la organización, ya sea propiedad de la empresa o de terceros.

3. RESPONSABILIDADES

3.1. Responsable de Seguridad de la Información

El responsable de seguridad de la información tiene la responsabilidad de:

Coordinar y supervisar el proceso de gestión de la información secreta de autenticación de los usuarios.
Establecer y mantener políticas y procedimientos para el manejo seguro de la información secreta de autenticación.
Implementar controles adecuados para proteger la información secreta de autenticación.

3.2 Usuarios

Los usuarios tienen la responsabilidad de:

Utilizar la información secreta de autenticación asignada de manera segura y confidencial.
Cumplir con las políticas y procedimientos establecidos para la gestión de la información secreta de autenticación.
Informar cualquier sospecha de pérdida, robo o compromiso de la información secreta de autenticación al responsable de seguridad de la información.

4. PROCESO DE GESTION DE LA INFORMACIÓN SECRETA DE AUTENTICACIÓN DE LOS USUARIOS

5.

4.1 Generación y Entrega Segura de Claves Secretas

El responsable de seguridad de la información es el encargado de generar y distribuir de

manera segura las claves secretas y los métodos de autenticación de doble factor. Este proceso incluirá:

- Generación de claves de autenticación únicas y seguras mediante algoritmos criptográficos.
- Uso de plataformas seguras para la entrega de estas claves, como aplicaciones de autenticación que cumplen con los estándares de seguridad requeridos.
- Entrega física de dispositivos de autenticación de doble factor, como tokens de hardware, en un entorno controlado y registrando la cadena de custodia.

4.2 Almacenamiento Seguro de Claves Secretas

El almacenamiento de las claves secretas de autenticación de doble factor debe realizarse siguiendo prácticas de seguridad estrictas:

- Las claves almacenadas electrónicamente se cifrarán tanto en tránsito como en reposo.
- Los dispositivos físicos de autenticación de doble factor se guardarán en un lugar seguro y solo serán accesibles por el usuario autorizado.
- Se evitará el almacenamiento de claves secretas en texto plano o medios inseguros.

4.3 Actualización y Cambio Periódico de Claves Secretas

Es fundamental mantener la vigencia y efectividad de las claves secretas mediante su actualización periódica:

- Se establecerá una política de caducidad de claves que obligue a los usuarios a cambiar o actualizar su autenticación de doble factor regularmente.
- Se fomentará el uso de aplicaciones de autenticación que generen códigos de acceso dinámicos y temporales.

4.4 Respuesta a Incidentes y Recuperación de Claves Secretas

Se establecerán procedimientos claros y efectivos para la respuesta a incidentes relacionados con la autenticación de doble factor:

- En caso de pérdida o sospecha de compromiso de una clave secreta, se deberá reportar inmediatamente al departamento de seguridad de la información.
- Se implementará un proceso de revocación y reemisión rápida de claves secretas para mitigar posibles daños.
- Se realizarán auditorías de seguridad después de cualquier incidente para ajustar los procedimientos y prevenir futuros compromisos.

4.5 Capacitación y Concientización de Usuarios

Se proporcionará capacitación regular a los usuarios sobre la importancia y el uso adecuado de la autenticación de doble factor:

- Sesiones de formación sobre cómo gestionar y proteger las claves secretas.
- Distribución de material educativo que resalte las mejores prácticas y las políticas de la empresa.

6. REVISION Y MEJORA CONTINUA

Se realizarán revisiones periódicas del proceso de gestión de la información secreta de autenticación para identificar áreas de mejora y tomar las acciones correctivas correspondientes.

Se actualizará la documentación y las políticas según sea necesario para reflejar los cambios y requisitos actuales.

Este proceso de gestión de la información secreta de autenticación de los usuarios se considera parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) de CV CONSTRUCCIONES GENERALES S.A.C. El incumplimiento de este proceso puede resultar en medidas disciplinarias, según las políticas internas de la empresa y las leyes aplicables.

Procedimiento de MFA para proteger cuenta con la autenticación multifactor

CV CONSTRUCCIONES GENERALES S.A.C

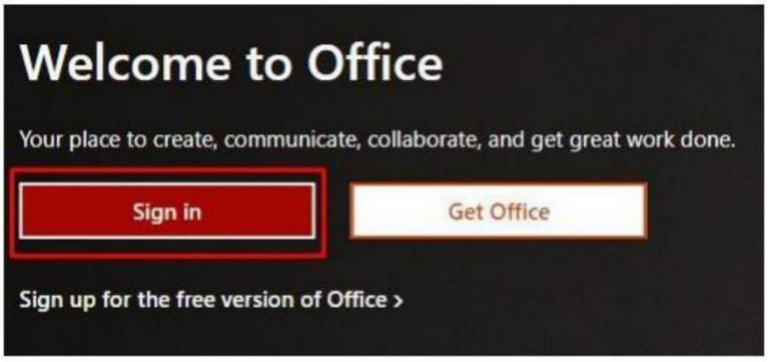
Universidad César Vallejo

Activación del Proceso de MFA

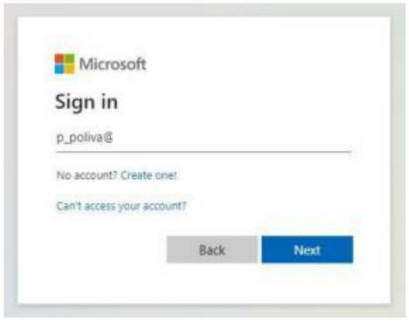
Para poder activar el protocolo MFA (Doble Factor), para los correos de acceso.

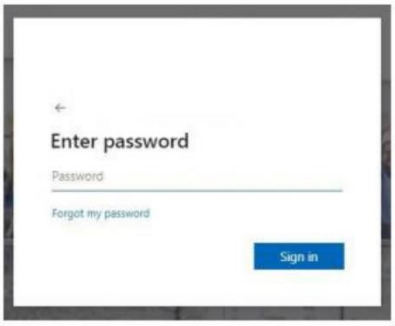
1. Se requiere ingresar al siguiente link: https://www.office.com/

2. Loguearte con la cuenta brindada:



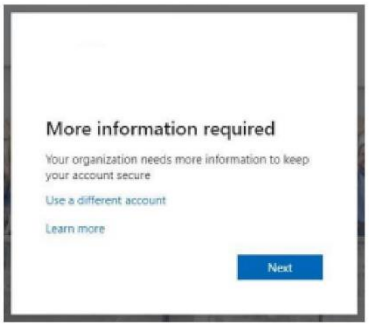
3. Tener en cuenta lo siguiente el correo se constituye de la siguiente manera “Usuario de red” y agregar el “@cvconstrucciones.com.pe”



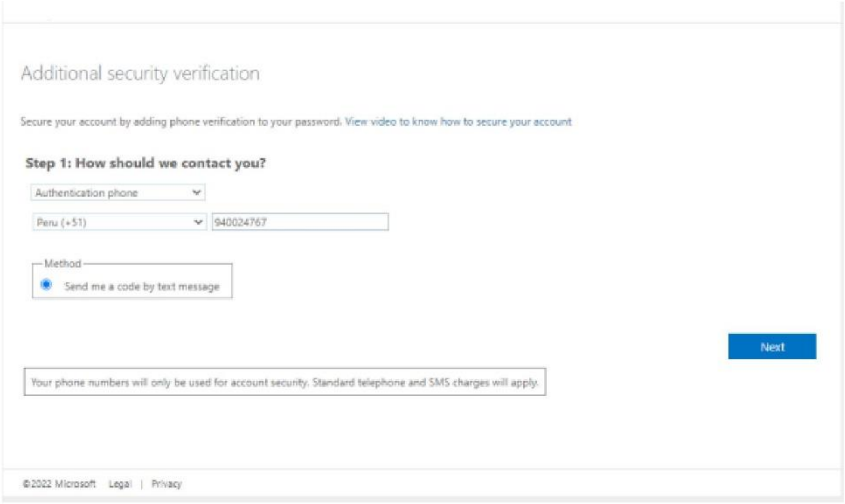


4. Colocar su contraseña de acceso, es la misma contraseña de la cuenta de red.

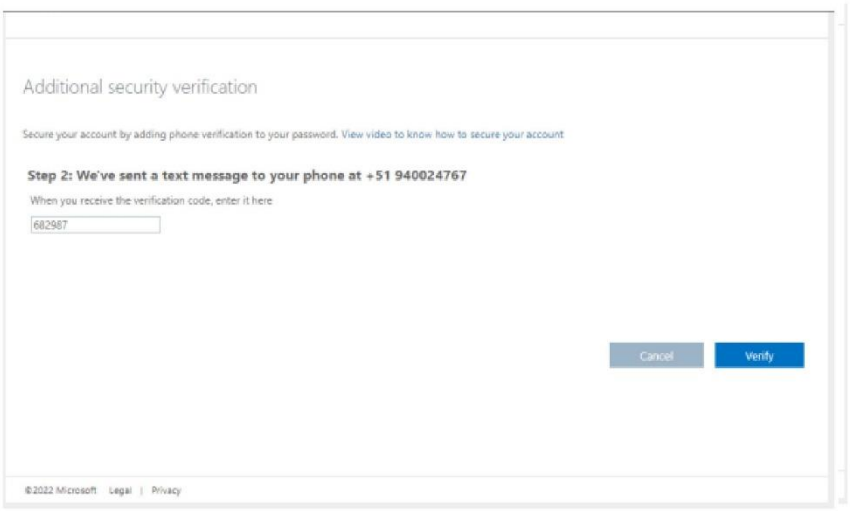
5. Nos mostrara la siguiente pantalla



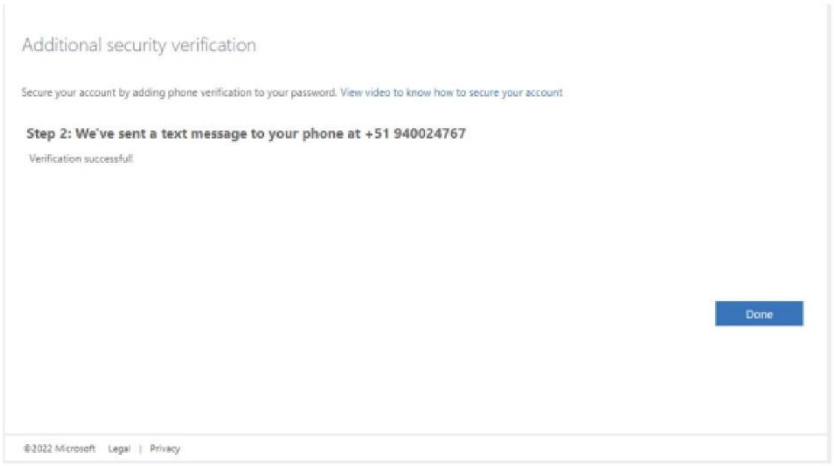
6. Presionar Next, en la nueva ventana se deberá agregar el numero al cual se enviará el SMS de validación para brindar el acceso.



7. Presionamos Next, esperamos el mensaje se registra el código y presionamos Verify.



8. Se presiona Done y el proceso se terminará.



9. Ahora cada vez que ingresen o usen el correo nos solicitara ingresar el código de confirmación.

10. Una vez confirmando nos permitirá ingresar.

ISO/IEC 27001:2013 – A.9.2.5 Revisión de los derechos de acceso de usuarios

1. OBJETIVO

El objetivo de este entregable es establecer un procedimiento para la verificación periódica de los derechos de acceso de los usuarios en los sistemas y servicios de tecnología de la información (TI) de CV CONSTRUCCIONES GENERALES S.A.C. La verificación de los derechos de acceso garantizará que los usuarios tengan los privilegios de acceso adecuados y autorizados, y ayudará a prevenir el acceso no autorizado y los posibles incidentes de seguridad.

2. ALCANCE

Este entregable se aplica a todos los empleados, contratistas y terceros que utilizan sistemas y servicios de TI de CV CONSTRUCCIONES GENERALES S.A.C. y tienen derechos de acceso a los mismos. También se extiende a cualquier recurso de TI utilizado en nombre de la organización, ya sea propiedad de la empresa o de terceros.

3. RESPONSABILIDADES

3.1. Responsable de Seguridad de la Información

El responsable de seguridad de la información tiene la responsabilidad de:

Coordinar y supervisar la verificación de los derechos de acceso de los usuarios.
Establecer y mantener políticas y procedimientos para la verificación de los derechos de acceso.
Realizar las verificaciones de los derechos de acceso según lo programado.

3.2. Responsables de los Sistemas y Servicios de TI

Los responsables de los sistemas y servicios de TI tienen la responsabilidad de:

Proporcionar al responsable de seguridad de la información la información actualizada sobre los derechos de acceso de los usuarios en sus sistemas y servicios.
Colaborar con el responsable de seguridad de la información durante las verificaciones de los derechos de acceso.

4. PROCESO DE VERIFICACIÓN DE LOS DERECHOS DE ACCESO DE LOS USUARIOS

4.1 Programación de Verificaciones

El responsable de seguridad de la información programará verificaciones periódicas de los derechos de acceso de los usuarios en todos los sistemas y servicios de TI de CV CONSTRUCCIONES GENERALES S.A.C.

La frecuencia de las verificaciones dependerá de la criticidad de los sistemas y servicios, así

como de las políticas y regulaciones aplicables.

4.2 Recopilación de Información

El responsable de seguridad de la información recopilará la información necesaria sobre los derechos de acceso de los usuarios en los sistemas y servicios de TI.

Se verificará la exactitud y actualidad de la información recopilada.

4.3 Comparación de Derechos de Acceso

Se compararán los derechos de acceso de los usuarios recopilados con los derechos de acceso autorizados y documentados.

Se identificarán y registrarán las discrepancias o desviaciones encontradas.

4.4 Acciones Correctivas

En caso de encontrar discrepancias o desviaciones en los derechos de acceso de los usuarios, se tomarán las acciones correctivas correspondientes.

Se comunicará con los responsables de los sistemas y servicios de TI para corregir y ajustar los derechos de acceso de los usuarios según sea necesario.

4.5 Documentación y Reporte

Se documentarán los resultados de la verificación de los derechos de acceso de los usuarios, incluyendo las acciones correctivas tomadas.

Se generará un informe que resuma los resultados de la verificación y se presentará al responsable de seguridad de la información.

5. REVISION Y MEJORA CONTINUA

Se realizarán revisiones periódicas de los procedimientos de verificación de los derechos de acceso de los usuarios para identificar áreas de mejora y tomar las acciones correctivas correspondientes.
Se actualizará la documentación y los procedimientos según sea necesario para reflejar los cambios y requisitos actuales.

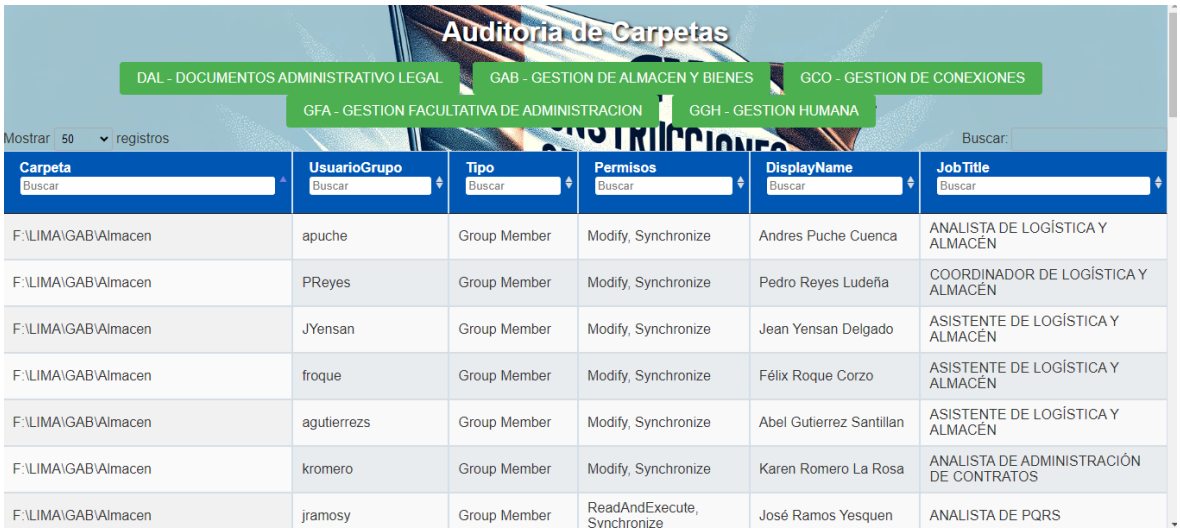
Este entregable de verificación de los derechos de acceso de los usuarios se considera parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) de CV

CONSTRUCCIONES GENERALES S.A.C. El incumplimiento de este entregable puede resultar en medidas disciplinarias, según las políticas internas de la empresa y las leyes aplicables.

Sistema implementado para la auditoria de repositorios

Estimados representantes de CV CONSTRUCCIONES GENERALES SAC

Con la presente, me permito dirigirme a ustedes para presentar el Sistema de Auditoria para el control de accesos a los repositorios.



Carpeta	UsuarioGrupo	Tipo	Permisos	DisplayName	JobTitle
F:\LIMA\GAB\Almacen	apuche	Group Member	Modify, Synchronize	Andres Puche Cuenca	ANALISTA DE LOGÍSTICA Y ALMACÉN
F:\LIMA\GAB\Almacen	PReyes	Group Member	Modify, Synchronize	Pedro Reyes Ludeña	COORDINADOR DE LOGÍSTICA Y ALMACÉN
F:\LIMA\GAB\Almacen	JYensan	Group Member	Modify, Synchronize	Jean Yensan Delgado	ASISTENTE DE LOGÍSTICA Y ALMACÉN
F:\LIMA\GAB\Almacen	froque	Group Member	Modify, Synchronize	Félix Roque Corzo	ASISTENTE DE LOGÍSTICA Y ALMACÉN
F:\LIMA\GAB\Almacen	agutierrezs	Group Member	Modify, Synchronize	Abel Gutierrez Santillan	ASISTENTE DE LOGÍSTICA Y ALMACÉN
F:\LIMA\GAB\Almacen	kromero	Group Member	Modify, Synchronize	Karen Romero La Rosa	ANALISTA DE ADMINISTRACIÓN DE CONTRATOS
F:\LIMA\GAB\Almacen	jramosy	Group Member	ReadAndExecute, Synchronize	José Ramos Yesquen	ANALISTA DE PQRS

Atentamente,

Christian Barrientos Inga

Estudiante de Ingeniería de Sistemas

Script basado en PowerShell para realizar la auditoria de repositorios

CV CONSTRUCCIONES GENERALES S.A.C

Universidad César Vallejo

Script (PowerShell para auditoria de Revisión de Acceso)

```
# Mensaje al inicio del script
Write-Host "SE INICIA ANÁLISIS DE AUDITORIA MENSUAL PARA CV CONSTRUCCIONES GENERALES S.A.C..... PROGRAMA EN PROGRESO" -ForegroundColor Red


# Definir función para obtener los permisos de una carpeta específica con un nivel máximo de profundidad
function Obtener-PermisosCarpeta {
    param ($ruta)
    Get-ChildItem -Path $ruta -Directory | ForEach-Object {
        $rutaCompleta = $_.FullName
        $acl = Get-Acl -Path $rutaCompleta
        foreach ($accessRule in $acl.Access) {
            $usuarioGrupo = $accessRule.IdentityReference.Value
            # Verificar si el usuario o grupo tiene permisos y si pertenece al dominio 'PERU'
            if ($usuarioGrupo -match "PERU\\") {
                [PSCustomObject]@{
                    Carpeta = $rutaCompleta
                    UsuarioGrupo = $usuarioGrupo -replace "^PERU\\", ""
                    Tipo = $accessRule.AccessControlType
                    Permisos = $accessRule.FileSystemRights
                }
            }
        }
    }
}


# Definir función para obtener usuarios de grupos recursivamente
function Obtener-UsuariosDeGrupo {
```

```
    param ($grupo)

    try {

        if ($grupo -eq "Domain Users") {
            # Si el grupo es "Domain Users", no hacemos nada y pasamos al siguiente grupo
            return @()
        }
        $miembros = Get-ADGroupMember -Identity $grupo | Where-Object { $_.objectClass -eq
"User" }
        return $miembros.SamAccountName
    } catch {
        # Manejo de la excepción, aquí simplemente la ignoramos o podríamos registrarla en un
archivo de log si se desea
        return @() # Devolvemos un array vacío si hay un error
    }
}

# Definir función para verificar si un usuario está habilitado en Active Directory
function Usuario-Habilitado {
    param ($usuario)
    try {
        if ($usuario -match "^G_" -or $usuario -eq "Domain Users") {
            # Los usuarios que comienzan con "G_" o son "Domain Users" se consideran habilitados
automáticamente
            return $true
        } else {
            $usuarioAD = Get-ADUser -Identity $usuario -Properties Enabled
            if ($usuarioAD.Enabled) {
                return $true
            } else {
```

```
            return $false
        }
    }
  } catch {
    return @() # Devolvemos un array vacío si hay un error
  }
}
# Definir función para ejecutar el script en la sesión remota y exportar los resultados
function Ejecutar-ScriptRemoto {
  param ($servidorRemoto, $rutaCarpetaPrincipal)
  # Credenciales y sesión remota
  $credenciales = New-Object System.Management.Automation.PSCredential(".\administrator",
(ConvertTo-SecureString "Peru2020$" -AsPlainText -Force))
  $sesion = New-PSSession -ComputerName $servidorRemoto -Credential $credenciales

  # Invocar función para obtener permisos y exportar resultados a un archivo CSV
  $usuarios = Invoke-Command -Session $sesion -ScriptBlock ${function:Obtener-
PermisosCarpeta} -ArgumentList $rutaCarpetaPrincipal

  # Obtener usuarios de grupos y añadirlos a la lista
  $usuariosConGrupos = @()
  foreach ($usuario in $usuarios) {
    $usuariosConGrupos += $usuario
    $usuariosDeGrupo = Obtener-UsuariosDeGrupo -grupo $usuario.UsuarioGrupo
    foreach ($usuarioDeGrupo in $usuariosDeGrupo) {
      $usuariosConGrupos += [PSCustomObject]@{
        Carpeta = $usuario.Carpeta
        UsuarioGrupo = $usuarioDeGrupo
        Tipo = "Group Member"
        Permisos = $usuario.Permisos
      }
```

```
    }
}

# Verificar si se encontraron resultados y si los usuarios están habilitados en AD
$usuariosHabilitados = @()
foreach ($usuario in $usuariosConGrupos) {
    if (Usuario-Habilitado -usuario $usuario.UsuarioGrupo) {
        $usuariosHabilitados += $usuario
    }
}

# Definir función para obtener información adicional del usuario
function Obtener-InformacionUsuario {
    param ($usuario)
    try {
        $usuarioAD = Get-ADUser -Identity $usuario -Properties DisplayName, Title, City,
Department, CanonicalName
        if ($usuarioAD) {
            return [PSCustomObject]@{
                Usuario = $usuarioAD.SamAccountName
                DisplayName = $usuarioAD.DisplayName
                JobTitle = $usuarioAD.Title
                City = $usuarioAD.City
                Department = $usuarioAD.Department
                CanonicalName = $usuarioAD.CanonicalName
            }
        } else {
            return @()
        }
    } catch {
        return @()
```

```
    }
  }

  # Verificar si se encontraron resultados y si los usuarios están habilitados en AD
  $usuariosConInformacion = @()
  foreach ($usuario in $usuariosHabilitados) {
    $infoUsuario = Obtener-InformacionUsuario -usuario $usuario.UsuarioGrupo
    if ($infoUsuario) {
      $usuariosConInformacion += $usuario | Add-Member -MemberType NoteProperty -Name
"DisplayName" -Value $infoUsuario.DisplayName -PassThru |
        Add-Member -MemberType NoteProperty -Name "JobTitle" -Value $infoUsuario.JobTitle
-PassThru |
        Add-Member -MemberType NoteProperty -Name "City" -Value $infoUsuario.City -
PassThru |
        Add-Member -MemberType NoteProperty -Name "Department" -Value
$infoUsuario.Department -PassThru |
        Add-Member -MemberType NoteProperty -Name "CanonicalName" -Value
$infoUsuario.CanonicalName -PassThru
    }
  }

  # Comentar la siguiente línea para evitar que se muestre en la consola
  # $usuariosConInformacion | Out-Null

  # Exportar resultados a un archivo CSV
  if ($usuariosHabilitados.Count -gt 0) {
    $usuariosHabilitados | Export-Csv -Path "$Env:USERPROFILE\Desktop\GCO.csv" -
NoTypeInformation -Encoding UTF8
  } else {
    return @()
  }

  # Cerrar la sesión remota
```

```
    Remove-PSSession -Session $sesion
}

# Llamar a la función para ejecutar el script en el servidor remoto con la ruta especificada
Ejecutar-ScriptRemoto -servidorRemoto "Slimfil01" -rutaCarpetaPrincipal "H:\GCO"

# Mensaje al final del script
Write-Host "SE COMPLETO EL ANÁLISIS Y SE EXPORTA EL REPORTE SOLICITADO PARA EL
EVALUACIÓN DEL ENCARGADO DE SGSI CHRISTIAN BARRIENTOS" -ForegroundColor Green
```

ISO/IEC 27001:2013 – A.9.2.6 Retiro o ajuste de los derechos de acceso

1. OBJETIVO

El objetivo de este entregable es establecer un procedimiento para el retiro o ajuste oportuno de los derechos de acceso de los usuarios en los sistemas y servicios de tecnología de la información (TI) de CV CONSTRUCCIONES GENERALES S.A.C. Este procedimiento garantizará que los usuarios tengan los privilegios de acceso adecuados y autorizados en todo momento, y ayudará a prevenir el acceso no autorizado y los posibles incidentes de seguridad.

2. ALCANCE

Este entregable se aplica a todos los empleados, contratistas y terceros que utilizan sistemas y servicios de TI de CV CONSTRUCCIONES GENERALES S.A.C. y tienen derechos de acceso a los mismos. También se extiende a cualquier recurso de TI utilizado en nombre de la organización, ya sea propiedad de la empresa o de terceros.

3. RESPONSABILIDADES

3.1 Responsable de Seguridad de la Información

El responsable de seguridad de la información tiene la responsabilidad de:

Coordinar y supervisar el proceso de retiro o ajuste de los derechos de acceso de los usuarios.
Establecer y mantener políticas y procedimientos para el retiro o ajuste de los derechos de acceso.
Realizar las acciones necesarias para retirar o ajustar los derechos de acceso según sea necesario.

3.2 Responsables de los Sistemas y Servicios de TI

Los responsables de los sistemas y servicios de TI tienen la responsabilidad de:

Notificar al responsable de seguridad de la información cuando sea necesario retirar o ajustar los derechos de acceso de los usuarios en sus sistemas y servicios.
Colaborar con el responsable de seguridad de la información durante el proceso de retiro o ajuste de los derechos de acceso.

4. PROCEDIMIENTO DE RETIRO O AJUSTE DE LOS DERECHOS DE ACCESO

4.1 Identificación de la Necesidad de Retiro o Ajuste

El responsable de seguridad de la información o los responsables de los sistemas y servicios de TI identificarán la necesidad de retirar o ajustar los derechos de acceso de los usuarios.

Esto puede ser resultado de cambios en los roles, responsabilidades o empleo del usuario, o como parte de la revisión periódica de los derechos de acceso.

4.2 Evaluación y Autorización

El responsable de seguridad de la información evaluará la necesidad de retirar o ajustar los derechos de acceso y obtendrá la autorización correspondiente.

Se verificará la justificación y se documentará el motivo del retiro o ajuste de los derechos de acceso.

4.3 Retiro o Ajuste de los Derechos de Acceso

Se llevarán a cabo las acciones necesarias para retirar o ajustar los derechos de acceso de los usuarios en los sistemas y servicios de TI.

Se seguirán los procedimientos y controles adecuados para garantizar la ejecución correcta y segura de las acciones.

4.4 Comunicación y Notificación

Se notificará al usuario afectado sobre el retiro o ajuste de sus derechos de acceso.

Se proporcionará la justificación y la información necesaria para cualquier ajuste realizado.

4.5 Documentación y Registro

Se documentará el retiro o ajuste de los derechos de acceso, incluyendo la justificación y las acciones realizadas.

Se mantendrán registros actualizados de los cambios realizados en los derechos de acceso de los usuarios.

Este entregable de retiro o ajuste de los derechos de acceso se considera parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) de CV CONSTRUCCIONES GENERALES S.A.C. El incumplimiento de este entregable puede resultar en medidas disciplinarias, según las políticas internas de la empresa y las leyes aplicables.

ISO/IEC 27001:2013 – A.9.3.1 Uso de información secreta de autenticación

1. OBJETIVO

El objetivo de este entregable es establecer un procedimiento para el uso adecuado de la información secreta de autenticación por parte de los usuarios en los sistemas y servicios de tecnología de la información (TI) de CV CONSTRUCCIONES GENERALES S.A.C. Este procedimiento garantizará que los usuarios sigan las prácticas establecidas por la organización para proteger la información secreta de autenticación y ayudará a prevenir el acceso no autorizado y los posibles incidentes de seguridad.

2. ALCANCE

Este entregable se aplica a todos los empleados, contratistas y terceros que utilizan sistemas y servicios de TI de CV CONSTRUCCIONES GENERALES S.A.C. y tienen acceso a la información secreta de autenticación. También se extiende a cualquier recurso de TI utilizado en nombre de la organización, ya sea propiedad de la empresa o de terceros.

3. RESPONSABILIDADES

3.1 Responsable de Seguridad de la Información

El responsable de seguridad de la información tiene la responsabilidad de:

Establecer y mantener políticas y prácticas para el uso adecuado de la información secreta de autenticación.
Comunicar y capacitar a los usuarios sobre las prácticas establecidas.
Supervisar y hacer cumplir el cumplimiento de las prácticas de uso de la información secreta de autenticación.

3.2 Usuarios

Los usuarios tienen la responsabilidad de:

Familiarizarse y cumplir con las políticas y prácticas establecidas para el uso de la información secreta de autenticación.
Utilizar la información secreta de autenticación de manera segura y responsable.
Informar cualquier incidente o sospecha de acceso no autorizado o compromiso de la información secreta de autenticación.

4. PROCEDIMIENTO DE USO DE INFORMACION SECRETA DE AUTENTICACIÓN

4.1 Comunicación y Capacitación

El responsable de seguridad de la información comunicará y capacitará a los usuarios sobre

las prácticas establecidas para el uso de la información secreta de autenticación.

Se proporcionará información sobre la importancia de proteger la información secreta de autenticación, las medidas de seguridad a seguir y las consecuencias del uso inadecuado.

4.2 Cumplimiento de las Prácticas Establecidas

Los usuarios deben seguir las prácticas establecidas por la organización para el uso de la información secreta de autenticación.

Esto incluye mantener la información secreta de autenticación confidencial, no compartirla con personas no autorizadas y no utilizarla de manera inapropiada o no autorizada.

4.3 Informe de Incidentes

Los usuarios deben informar de inmediato cualquier incidente o sospecha de acceso no autorizado o compromiso de la información secreta de autenticación al responsable de seguridad de la información.

Se seguirán los procedimientos establecidos para investigar y abordar los incidentes reportados.

4.4 Consecuencias del Uso Inadecuado

El incumplimiento de las prácticas establecidas para el uso de la información secreta de autenticación puede resultar en medidas disciplinarias, según las políticas internas de la empresa y las leyes aplicables.

5. REVISIÓN Y MEJORA CONTINUA

Se realizarán revisiones periódicas del procedimiento de uso de la información secreta de autenticación para identificar áreas de mejora y tomar las acciones correctivas correspondientes.

Se actualizará la documentación y los procedimientos según sea necesario para reflejar los cambios y requisitos actuales.

Este entregable de uso de información secreta de autenticación se considera parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) de CV CONSTRUCCIONES GENERALES S.A.C. El incumplimiento de este entregable puede resultar en medidas disciplinarias, según las políticas internas de la

Evidencia de las capacitaciones

ISO/IEC 27001:2013 – A.9.4.1 Restricción del acceso a la información

1. OBJETIVO

El objetivo de este entregable es establecer un procedimiento para restringir el acceso a la información y a las funciones de aplicación del sistema de acuerdo con la política de control de acceso en CV CONSTRUCCIONES GENERALES S.A.C. Este procedimiento garantizará que se implementen las medidas necesarias para proteger la información confidencial y restringir el acceso no autorizado a los sistemas y datos de la organización.

2. ALCANCE

Este entregable se aplica a todos los empleados, contratistas y terceros que tienen acceso a los sistemas y datos de CV CONSTRUCCIONES GENERALES S.A.C. y se extiende a cualquier recurso de TI utilizado en nombre de la organización, ya sea propiedad de la empresa o de terceros.

3. RESPONSABILIDADES

3.1 Responsable de Seguridad de la Información

El responsable de seguridad de la información tiene la responsabilidad de:

Establecer y mantener la política de control de acceso, que incluye la restricción del acceso a la información y a las funciones de aplicación del sistema.
Definir los roles y permisos de acceso según las necesidades del negocio y los principios de mínimos privilegios.
Supervisar y hacer cumplir el cumplimiento de las políticas y controles de acceso.

3.2 Administradores del Sistema

Los administradores del sistema tienen la responsabilidad de:

Implementar y mantener las medidas técnicas y de seguridad necesarias para restringir el acceso a la información y a las funciones de aplicación del sistema.
Asignar y gestionar los permisos de acceso de acuerdo con las políticas y requisitos establecidos.
Supervisar y revisar regularmente los permisos de acceso para asegurarse de que sean adecuados y estén actualizados.

3.2 Usuarios

Los usuarios tienen la responsabilidad de:

Utilizar los sistemas y datos de manera responsable y conforme a su rol y permisos de acceso asignados.
No compartir sus credenciales de acceso con personas no autorizadas.
Informar cualquier incidente o sospecha de acceso no autorizado o inapropiado al responsable de seguridad de la información.

4. PROCEDIMIENTO DE RESTRICCION DEL ACCESO A LA INFORMACIÓN

4.1 Definición de Roles y Permisos de Acceso

El responsable de seguridad de la información junto con los administradores del sistema definirá los roles y permisos de acceso basados en las necesidades del negocio y los principios de mínimos privilegios.
Se establecerá una matriz de permisos que indique qué funciones y datos puede acceder cada rol.

4.2 Asignación y Gestión de Permisos de Acceso

Los administradores del sistema serán responsables de asignar los permisos de acceso a los usuarios de acuerdo con los roles establecidos.

Se implementarán medidas para asegurar que los cambios en los permisos de acceso se realicen de manera controlada y documentada.

4.3 Supervisión y Revisión de los Permisos de Acceso

Se llevará a cabo una supervisión regular de los permisos de acceso para asegurarse de que sean adecuados y estén actualizados.

Se realizarán revisiones periódicas de los permisos de acceso para garantizar que se sigan los principios de mínimos privilegios y eliminar cualquier acceso no necesario.

4.4 Cumplimiento de la Política de Control de Acceso

Todos los usuarios deben cumplir con la política de control de acceso establecida por la organización.

El incumplimiento de la política puede resultar en medidas disciplinarias, según las políticas internas de la empresa y las leyes aplicables.

5. REVISIÓN Y MEJORA CONTINUA

Se realizarán revisiones periódicas del procedimiento de restricción del acceso para identificar

áreas de mejora y tomar las acciones correctivas correspondientes.

Se actualizará la documentación y los procedimientos según sea necesario para reflejar los cambios y requisitos actuales.

Este entregable de restricción del acceso a la información se considera parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) de CV CONSTRUCCIONES GENERALES S.A.C. El incumplimiento de este entregable puede resultar en medidas disciplinarias, según las políticas internas de la empresa y las leyes aplicables.

ISO/IEC 27001:2013 – A.9.4.2 Procedimiento seguro de inicio de sesión

1. OBJETIVO

El objetivo de este entregable es establecer un procedimiento seguro de logeo para controlar el acceso a los sistemas y aplicaciones en CV CONSTRUCCIONES GENERALES S.A.C. Este procedimiento garantizará que los usuarios inicien sesión de manera segura, se autentiquen correctamente y se implementen medidas de protección para prevenir el acceso no autorizado a los sistemas y datos de la organización.

2. ALCANCE

Este entregable se aplica a todos los empleados, contratistas y terceros que tienen acceso a los sistemas y aplicaciones de CV CONSTRUCCIONES GENERALES S.A.C., ya sea de manera remota o en las instalaciones de la empresa.

3. RESPONSABILIDADES

3.1 Responsable de Seguridad de la Información

El responsable de seguridad de la información tiene la responsabilidad de:

Establecer y mantener el procedimiento seguro de logeo, que incluye las mejores prácticas de autenticación y control de acceso.
Comunicar y capacitar a los usuarios sobre el procedimiento seguro de logeo.
Supervisar y hacer cumplir el cumplimiento del procedimiento de logeo seguro.

3.2 Administradores del Sistema

Los administradores del sistema tienen la responsabilidad de:

Configurar y mantener los controles de seguridad relacionados con el logeo, como contraseñas, autenticación multifactor, bloqueo de cuentas por intentos fallidos, entre otros.

Monitorear los registros de logeo para detectar actividades sospechosas o intentos de acceso no autorizado.

Responder y manejar adecuadamente cualquier incidente de seguridad relacionado con el logeo.

3.2 Usuarios

Los usuarios tienen la responsabilidad de:

Seguir el procedimiento seguro de logeo establecido por la organización.

Utilizar contraseñas fuertes y únicas para sus cuentas.

Mantener la confidencialidad de sus credenciales de logeo y no compartirlas con personas no autorizadas.

Informar cualquier incidente o sospecha de acceso no autorizado o uso inapropiado de las cuentas.

4. PROCEDIMIENTO SEGURO DE LOGEO

4.1 Requisitos de Contraseñas

Los usuarios deben seguir las políticas establecidas para la creación de contraseñas seguras.

Se requerirá una combinación de caracteres alfanuméricos y especiales, una longitud mínima y cambios regulares de contraseña.

4.2 Autenticación Multifactor

Se implementará la autenticación multifactor en los sistemas y aplicaciones críticas.

Los usuarios deberán proporcionar una segunda forma de autenticación, como un código enviado a su teléfono móvil, junto con su contraseña.

4.3 Bloqueo de Cuentas por Intentos Fallidos

Se establecerá un mecanismo de bloqueo de cuentas después de un número predefinido de intentos fallidos de logeo.

Los usuarios deberán ponerse en contacto con el administrador del sistema para desbloquear sus cuentas.

4.4 Registros de Logeo y Monitoreo

Se habilitará el registro de eventos de logeo en los sistemas y aplicaciones.

Los administradores del sistema realizarán un monitoreo regular de los registros de logeo para detectar actividades sospechosas o intentos de acceso no autorizado.

5. REVISIÓN Y MEJORA CONTINUA

Se realizarán revisiones periódicas del procedimiento seguro de logeo para identificar áreas de mejora y tomar las acciones correctivas correspondientes.

Se actualizará la documentación y los procedimientos según sea necesario para reflejar los cambios y requisitos actuales.

Este entregable de procedimiento seguro de logeo se considera parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) de CV CONSTRUCCIONES GENERALES S.A.C. El incumplimiento de este entregable puede resultar en medidas disciplinarias, según las políticas internas de la empresa y las leyes aplicables.

Procedimiento de monitoreo de cuentas con el uso de Azure AD

CV CONSTRUCCIONES GENERALES S.A.C

Universidad César Vallejo

Monitoreo de cuentas desde Portal Azure

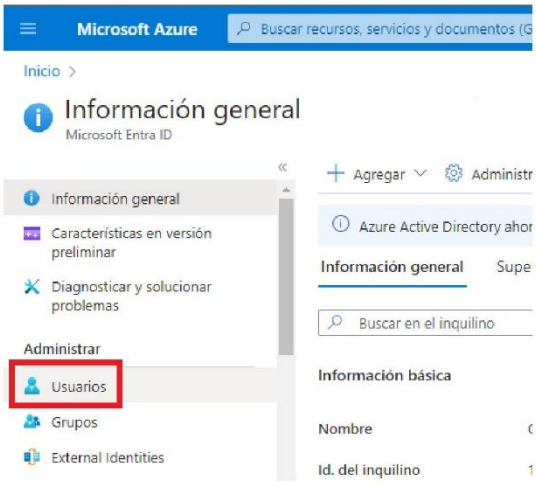
Para poder activar el protocolo MFA (Doble Factor), para los correos de acceso.

1. Se requiere ingresar al siguiente link: https://portal.azure.com/#home

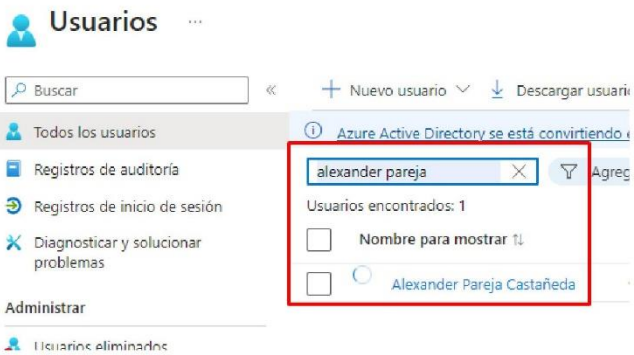
2. Loguearte con la cuenta brindada

3. Luego se debe dirigir al Microsoft Entra ID

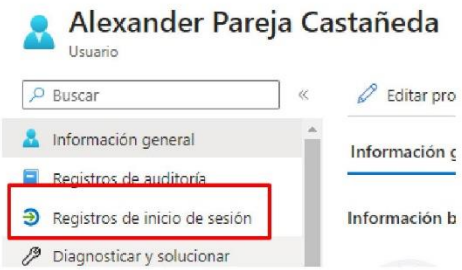
3. Nos vamos a la sección de Usuarios



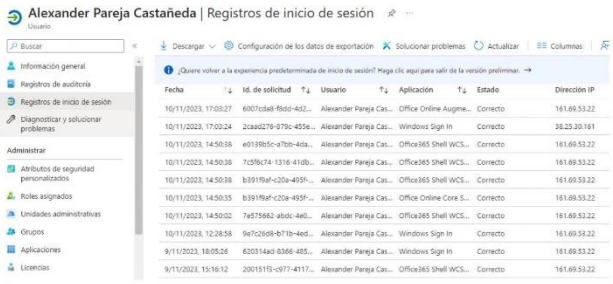
4. Buscamos al usuario a monitorear.



5. Nos dirigimos a Registro de Inicio de sesión



6. Vamos a visualizar los inicios de sesión, como parte de Auditoria.



ISO/IEC 27001:2013 – A.9.4.3 Sistema de gestión de claves

1. **OBJETIVO**

   El objetivo de este entregable es establecer un sistema de gestión de la clave y que asegure la calidad de las claves en CV CONSTRUCCIONES GENERALES S.A.C. Este sistema garantizará la seguridad y confidencialidad de las claves utilizadas en los sistemas y aplicaciones de la organización, así como la implementación de medidas para prevenir el acceso no autorizado a los datos sensibles.

2. **ALCANCE**

   Este entregable se aplica a todas las claves utilizadas en los sistemas y aplicaciones de CV CONSTRUCCIONES GENERALES S.A.C., incluyendo contraseñas, claves de cifrado y cualquier otro tipo de clave o credencial utilizada para acceder a los recursos protegidos.

3. **RESPONSABILIDADES**

   3.1 Responsable de Seguridad de la Información

   El responsable de seguridad de la información tiene la responsabilidad de:

   Establecer y mantener el sistema de gestión de la clave, que incluye políticas, procedimientos y controles relacionados con la generación, distribución, almacenamiento, uso y destrucción de las claves.

   Supervisar y hacer cumplir el cumplimiento del sistema de gestión de la clave.

   3.2 Administradores del Sistema

   Los administradores del sistema tienen la responsabilidad de:

   Implementar y mantener los controles técnicos necesarios para asegurar la calidad de las claves, como algoritmos de cifrados seguros, mecanismos de generación aleatoria y protección de claves en tránsito y en reposo.

   Gestionar el ciclo de vida de las claves, incluyendo la generación, distribución, almacenamiento y destrucción adecuada.

   3.3 Usuarios

   Los usuarios tienen la responsabilidad de:

   Utilizar las claves asignadas de acuerdo con las políticas y procedimientos establecidos.

   Mantener la confidencialidad de las claves y no compartirlas con personas no autorizadas.

Informar cualquier incidente o sospecha de acceso no autorizado o uso inapropiado de las claves.

4. SISTEMA DE GESTION DE LA CLAVE

4.1 GENERACIÓN DE CLAVES

Las claves se generarán utilizando algoritmos de cifrado seguros y mecanismos de generación aleatoria.

Se seguirán las mejores prácticas para garantizar la calidad y fortaleza de las claves generadas.

4.2 Distribución de Claves

Las claves se distribuirán de manera segura a los usuarios autorizados utilizando canales protegidos, como cifrado de extremo a extremo.

4.3 Almacenamiento de Claves

Las claves se almacenarán de manera segura utilizando mecanismos de protección adecuados, como almacenamiento cifrado y control de acceso basado en roles.

4.4 Uso de Claves

Los usuarios deben utilizar las claves asignadas de acuerdo con las políticas y procedimientos establecidos.

Se implementarán controles para prevenir el uso de claves débiles o comprometidas.

4.5 Criterio para la creación de contraseña

El uso de contraseñas en CV CONSTRUCCIONES GENERALES S.A.C. debe tomar en cuenta los siguientes criterios:

- Cantidad mínima de caracteres: 8
- Numero de intentos fallidos: 3
- Máximo tiempo de duración: 90 días
- Mínimo tiempo de duración: 1 día
- Historial de contraseñas: 8 contraseñas
- Bloqueo de contraseña tras intentos fallidos: 30 minutos
- Se deberá considerar una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (@, %, &, etc.)

5. REVISIÓN Y MEJORA CONTINUA

Se realizarán revisiones periódicas del sistema de gestión de la clave para identificar áreas de mejora y tomar las acciones correctivas correspondientes.

Se actualizará la documentación y los procedimientos según sea necesario para reflejar los cambios y requisitos actuales.

Este entregable del sistema de gestión de la clave se considera parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) de CV CONSTRUCCIONES GENERALES S.A.C. El incumplimiento de este entregable puede resultar en medidas disciplinarias, según las políticas internas de la empresa y las leyes aplicables.

Configuración de GPO en Windows Server para gestión de contraseñas de usuarios

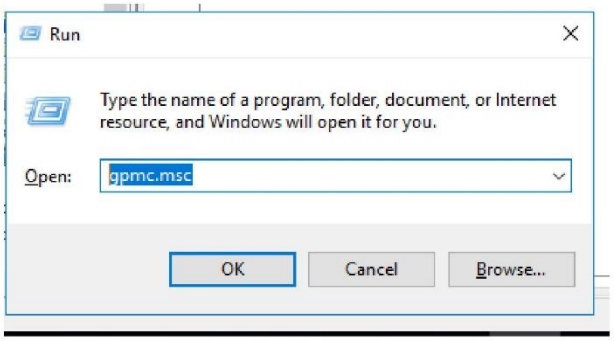
CV CONSTRUCCIONES GENERALES S.A.C

Universidad César Vallejo

Configuración de Política de Contraseña Por medio de GPO

1. Se requiere ingresar al controlador del dominio (SLIMDOM01)

2. Abrir Ejecutar y escribir gpmc.msc



3. Se abrirá el Group Policy Management.

4. Creamos una nueva política con el nombre de: SGSI POLITICA DE CONTRASEÑAS

5. Luego se abrirá el Gropup Policy Management Editor y procedemos a configurar.

6. Seguimos los pasos:

- Computer Configuration

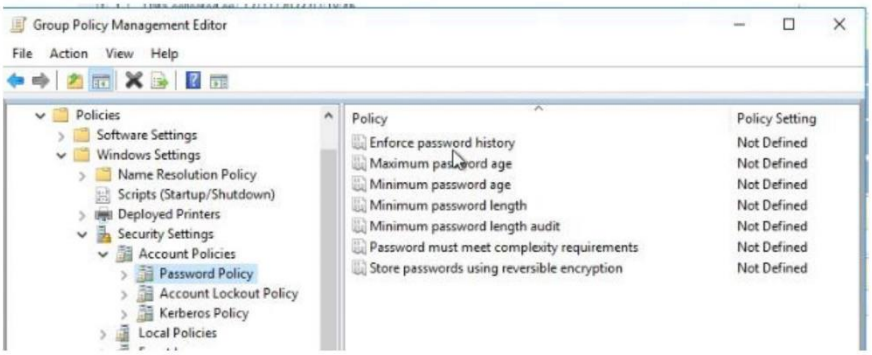
- Policies

- Windows Settings

- Securiy Settings

- Account Policies

- Password Policy



4. Configuramos como la política establecida en el documento SGSI POL 12

El uso de contraseñas en CV CONSTRUCCIONES GENERALES S.A.C. debe tomar en cuenta los siguientes criterios:

– Cantidad mínima de caracteres: 8

– Numero de intentos fallidos: 3

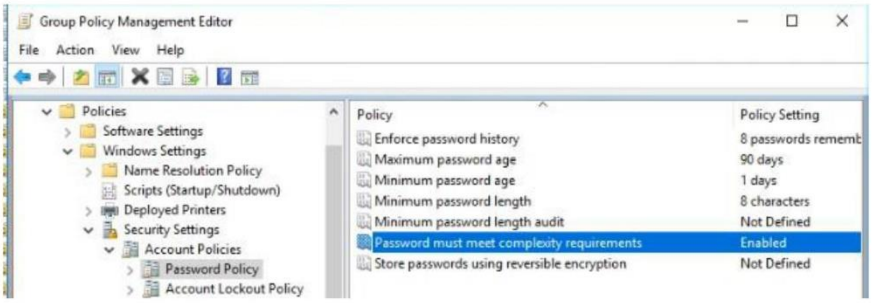
– Máximo tiempo de duración: 90 días

– Mínimo tiempo de duración: 1 día

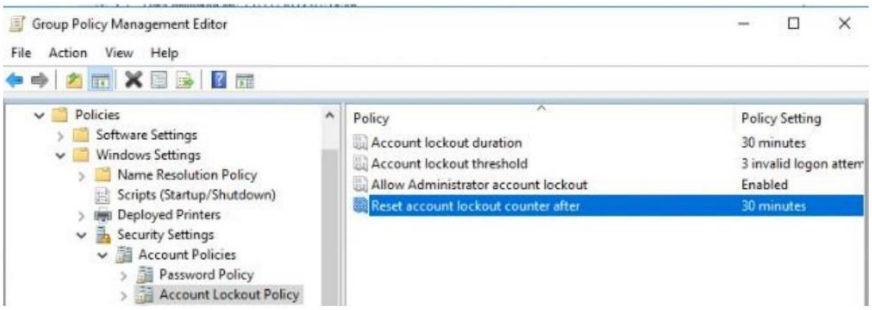
– Historial de contraseñas: 8 contraseñas

– Bloqueo de contraseña tras intentos fallidos: 30 minutos

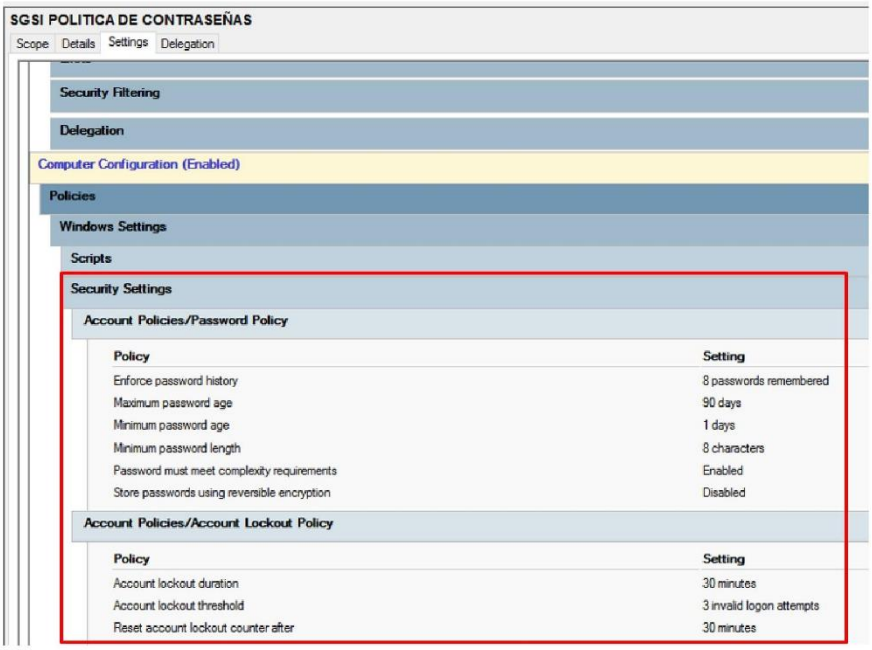
– Se deberá considerar una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (@, %, &, etc.)



5. Para las condiciones de bloqueo de cuenta, nos dirigimos a Account Lockout Policy



6. y Aplicamos.



SGSI POLITICA DE CONTRASEÑAS

Scope | Details | Settings | Delegation

Security Filtering

Delegation

Computer Configuration (Enabled)

Policies

Windows Settings

Scripts

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	8 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

ISO/IEC 27001:2013 – A.9.4.4 Uso de programas utilitarios de privilegio

1. OBJETIVO

El objetivo de este entregable es establecer controles para restringir y controlar severamente el uso de programas utilitarios que puedan controlar manualmente el sistema y los controles de la aplicación en CV CONSTRUCCIONES GENERALES S.A.C. Estos controles asegurarán que el acceso a programas utilitarios con privilegios esté limitado a personal autorizado y que se implementen medidas para prevenir el acceso no autorizado y el uso inapropiado de estos programas.

2. ALCANCE

Este entregable se aplica a todos los programas utilitarios que tienen la capacidad de controlar manualmente el sistema y los controles de la aplicación en CV CONSTRUCCIONES GENERALES S.A.C. Esto incluye programas utilitarios de administración de sistemas, herramientas de hacking ético y cualquier otro software similar con funciones de alto privilegio.

3. RESPONSABILIDADES

3.1 Responsable de Seguridad de la Información

El responsable de seguridad de la información tiene la responsabilidad de:

Establecer y mantener los controles para restringir y controlar el uso de programas utilitarios de privilegio.

Establecer políticas y procedimientos claros para el uso de programas utilitarios y la asignación de privilegios.

Supervisar y hacer cumplir el cumplimiento de los controles establecidos.

3.2 Administradores del Sistema

Los administradores del sistema tienen la responsabilidad de:

Controlar y restringir el acceso a los programas utilitarios de privilegio.

Asignar privilegios de manera adecuada y solo a personal autorizado.

Monitorear y auditar el uso de los programas utilitarios para detectar actividades sospechosas o uso inapropiado.

3.3 Usuarios

Los usuarios tienen la responsabilidad de:

Utilizar los programas utilitarios únicamente para fines autorizados y dentro del alcance de sus funciones.

No instalar o utilizar programas utilitarios no autorizados en los sistemas de la empresa.

Informar cualquier incidente o sospecha de acceso no autorizado o uso inapropiado de programas utilitarios.

4. CONTROLES PARA EL USO DE PROGRAMA UTILITARIOS DE PRIVILEGIO

4.1 Restricción de Acceso

El acceso a los programas utilitarios de privilegio estará restringido a personal autorizado y debidamente capacitado.

Se implementarán controles de acceso basados en roles y privilegios para limitar el uso de estos programas a las funciones y responsabilidades asignadas.

4.2 Monitoreo y Auditoría

Se realizará un monitoreo regular y una auditoría de los registros de uso de programas utilitarios de privilegio.

Los registros serán revisados para detectar actividades sospechosas o uso inapropiado, y se tomarán las acciones correctivas correspondientes.

4.3 Capacitación y Concientización

Se proporcionará capacitación regular sobre el uso adecuado de los programas utilitarios de privilegio y la importancia de su uso restringido.
Los usuarios serán conscientes de las políticas y procedimientos establecidos y de las consecuencias del uso no autorizado o inapropiado de estos programas.

4.4 Uso de Claves

Los usuarios deben utilizar las claves asignadas de acuerdo con las políticas y procedimientos establecidos.

Se implementarán controles para prevenir el uso de claves débiles o comprometidas.

5. REVISIÓN Y MEJORA CONTINUA

Se realizarán revisiones periódicas de los controles establecidos para restringir y controlar el uso de programas utilitarios de privilegio.

Se actualizará la documentación y los procedimientos según sea necesario para reflejar los cambios y requisitos actuales.

Este entregable sobre el uso de programas utilitarios de privilegio se considera parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) de CV CONSTRUCCIONES GENERALES S.A.C. El incumplimiento de este entregable puede resultar en medidas disciplinarias, según las políticas internas de la empresa y las leyes aplicables.

Configuración de los scripts desarrollados para uso solo de administradores

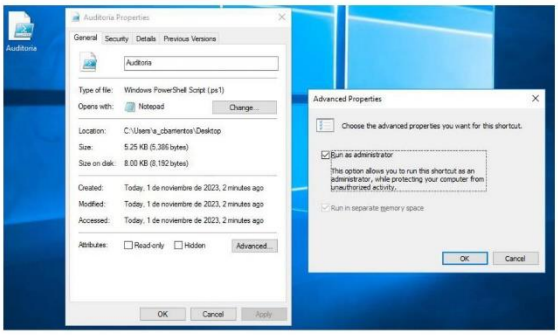
CV CONSTRUCCIONES GENERALES S.A.C

Universidad César Vallejo

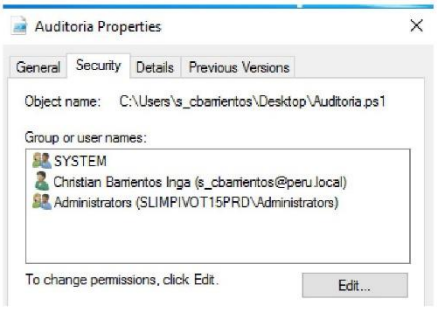
Configuración de programas con privilegio

1. Primero el uso de Script de PowerShell, debe ejecutar solo como administrador.

Para ello vamos a propiedades del archivo, opciones avanzadas y seleccionamos “ejecutar como administrador”

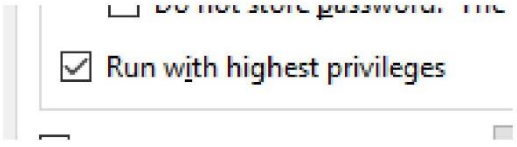


2.- Vamos a propiedades y vamos a la pestaña Seguridad y en Edit, solo brindamos permisos a las personas con los privilegios para el uso del Script



3. Para la ejecución de tareas programadas para el uso de este Script

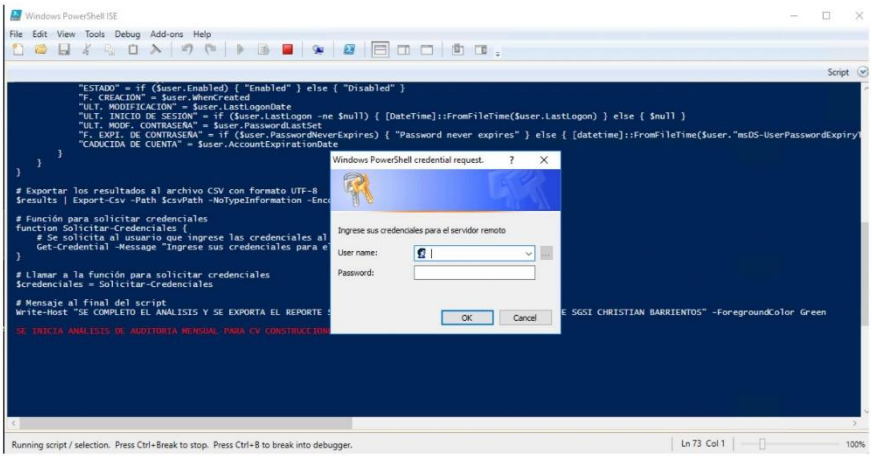
Al momento de programar una tarea de Windows, debe seleccionar, run with higthest privileges. Esto indica que solo se debe programar y ejecutar con permisos elevados.

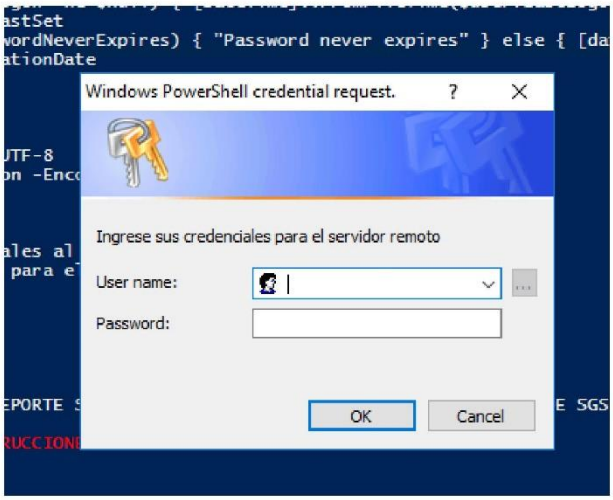


4.- Para el uso de Script para auditorias se implementará el comando:

Get-Credential

Para mejorar la seguridad y evitar incluir la contraseña en el script, se modificará la sección de credenciales para solicitar la contraseña al usuario administrador en tiempo de ejecución. Esto se hará con cmdlet **Get-Credential**, que muestra un cuadro de diálogo solicitando al usuario que ingrese su nombre de usuario y contraseña





ISO/IEC 27001:2013 – A.9.4.5 Control de acceso para programar el código fuente

1. OBJETIVO

El objetivo de este entregable es establecer controles para restringir el acceso al programa de código fuente en CV CONSTRUCCIONES GENERALES S.A.C. Estos controles garantizarán la confidencialidad e integridad del código fuente utilizado en los sistemas y aplicaciones de la organización, evitando el acceso no autorizado y protegiendo la propiedad intelectual

2. ALCANCE

Este entregable se aplica a todos los programas de código fuente utilizados en los sistemas y aplicaciones de CV CONSTRUCCIONES GENERALES S.A.C., incluyendo aquellos desarrollados internamente y aquellos adquiridos de terceros.

3. RESPONSABILIDADES

3.1 Responsable de Seguridad de la Información

El responsable de seguridad de la información tiene la responsabilidad de:

- Establecer y mantener controles para restringir el acceso al programa de código fuente.
- Definir y mantener una política de control de acceso al código fuente.
- Supervisar y hacer cumplir el cumplimiento de los controles establecidos.

3.2 Desarrolladores de Software

Los desarrolladores de software tienen la responsabilidad de:

- Acceder y utilizar el programa de código fuente únicamente para fines autorizados y dentro del alcance de sus funciones.
- Seguir las políticas y procedimientos establecidos para el control de acceso al código fuente.
- Informar cualquier incidente o sospecha de acceso no autorizado o uso inapropiado del código fuente.

4. CONTROLES PARA EL ACCESO AL PROGRAMA DE CÓDIGO FUENTE

4.1 Política de Control de Acceso

- Se establecerá una política de control de acceso al programa de código fuente que defina quiénes tienen acceso, los niveles de acceso permitidos y los procedimientos para solicitar acceso.

4.2 Gestión de Usuarios y Roles

- Se implementará un sistema de gestión de usuarios y roles para asignar y controlar los

privilegios de acceso al programa de código fuente.

- Los privilegios se asignarán de acuerdo con los roles y responsabilidades de cada usuario.

4.3 Autenticación y Autorización

- Se implementará un mecanismo de autenticación sólido para verificar la identidad de los usuarios que acceden al programa de código fuente.
- Se establecerán controles de autorización para garantizar que los usuarios solo tengan acceso a los componentes del código fuente necesarios para realizar sus funciones.

4.4 Seguimiento y Auditoría

- Se registrarán y monitorearán los accesos al programa de código fuente.
- Se realizarán auditorías regulares para detectar y analizar cualquier actividad sospechosa o acceso no autorizado.
-

5. REVISIÓN Y MEJORA CONTINUA

Se realizarán revisiones periódicas de los controles establecidos para restringir el acceso al programa de código fuente.

Se actualizará la documentación y los procedimientos según sea necesario para reflejar los cambios y requisitos actuales.

Este entregable sobre el control del acceso para programar el código fuente se considera parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) de CV CONSTRUCCIONES GENERALES S.A.C. El incumplimiento de este entregable puede resultar en medidas disciplinarias, según las políticas internas de la empresa y las leyes aplicables.

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, NECOCHEA CHAMORRO JORGE ISAAC, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Sistema de gestión de Control de Accesos basados en la ISO 27001:2013 para proteger la seguridad de información de CV Construcciones Generales SAC", cuyo autor es BARRIENTOS INGA CHRISTIAN SANTOS, constato que la investigación tiene un índice de similitud de 7.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 27 de Noviembre del 2023

Apellidos y Nombres del Asesor:	**Firma**
NECOCHEA CHAMORRO JORGE ISAAC **DNI:** 18167347 **ORCID:** 0000-0002-3290-8975	Firmado electrónicamente por: JNECOCHEA el 28-11-2023 09:20:27

Código documento Trilce: TRI - 0667544

INVESTIGA UCV