UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

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

TEMA:

ANÁLISIS E IMPLEMENTACIÓN DE LA CERTIFICACIÓN BASC EN UNA EMPRESA DE SERVICIOS ELECTRÓNICOS

AUTOR:

JOSÉ GERARDO ORTIZ CEVALLOS

DIRECTOR:

MIGUEL ÁNGEL QUIROZ MARTÍNEZ

CUENCA – ECUADOR

2026

Autor:

José Gerardo Ortiz Cevallos
Ingeniero en Electrónica.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
jortizce@est.ups.edu.ec

Dirigido por:

Miguel Ángel Quiroz Martínez
Ingeniero de Sistemas.
Máster en Ciencias y Tecnologías de la Computación.
mquiroz@ups.edu.ec

DEDICATORIA

Este es un logro cumplido con la convicción de siempre ser mejor y crecer en todos los sentidos, es lo que me enseñó Gerardo Ortiz Reyes mi papá que, aunque ya no está cerca, su legado siempre me guiará en el camino. Este trabajo es dedicado a él y a mi hija Dalia, que llegó a mi vida durante este proceso de maestría y hoy es mi motivo de seguir soñando y luchando por cumplir mis sueños y ahora también los suyos.

AGRADECIMIENTO

Si hay alguien a quien agradecer es a mi mamá, Elena Cevallos Cabrera, que siempre ha creído en mí y desde niño siempre ha estado a mi lado en todas las etapas de mi vida y es quien me ha llevado hasta aquí. También a mi familia que siempre son ese apoyo en los momentos difíciles y a mi mujer Johanna, que me ha acompañado en este proceso.

Tabla de Contenido

Análisis e Implementación de la Certificación BASC en una Empresa de Servicios Electrónicos

Autor(es):

José Gerardo Ortiz Cevallos

Resumen

En el presente documento, se analiza desarrolla el proceso de certificación BASC V6 en el apartado de Seguridad de la Información para una Empresa de Servicios Electrónicos, cuyas operaciones comerciales están enfocadas a la venta y arriendo de equipos informáticos a nivel nacional, y que, con la finalidad de mejorar su imagen institucional y así fortalecer lazos comerciales. En primera instancia, se analiza y describe el proceso documental que la empresa debe presentar para el cumplimiento con la Norma en la etapa de Certificación, posteriormente, se analizan los controles que solicita el estándar, se valida su cumplimiento en la matriz de control SGCS-BASC y se desarrollan las medidas de remediación para corregir las no conformidades, de forma que la empresa presenta la conformidad en el total de los controles, que engloban la parte tecnológica y humana, enfocando el componente de mejora continua en la capacitación del personal desarrollando su capacidad de respuesta ante amenazas, de esta forma la empresa garantiza que sus medidas de protección sean cada vez más robustas y se puedan mantenga su efectividad en el tiempo.

Al final de este documento, se presentan los controles implementados para la empresa de Servicios Electrónicos obteniendo una conformidad del 100% en la matriz de control del SGCS-BASC reduciendo los riesgos asociados a las no conformidades y el índice de mejora de respuesta que obtiene personal ante amenazas a la infraestructura tecnológica.

Palabras clave:

Certificación BASC V6, Seguridad de la Información, Gestión de Riesgos.

ABSTRACT

This document analyzes and develops the BASC V6 certification process in the Information Security section for an Electronic Services Company whose commercial operations are focused on the sale and leasing of computer equipment nationwide, with the aim of improving its institutional image and thus strengthening commercial ties. First, the document process that the company must submit to comply with the Standard in the Certification stage is analyzed and described. Subsequently, the controls required by the standard are analyzed, their compliance is validated in the SGCS-BASC control matrix, and remediation measures are developed to correct non-conformities, so that the company demonstrates compliance with all controls, encompassing both technological and human aspects, focusing on the component of continuous improvement in staff training, developing their ability to respond to threats. In this way, the company ensures that its protection measures are increasingly robust and can maintain their effectiveness over time.

At the end of this document, the controls implemented for the electronic services company are presented, achieving 100% compliance in the SGCS-BASC control matrix, reducing the risks associated with non-compliance and improving the response rate of personnel to threats to the technological infrastructure.

Palabras clave:
BASC V6 Certification, Information Security, Risk management.

1 Introducción

En un entorno marcado por la globalización y por crecientes exigencias en la protección de la cadena de suministro, las organizaciones deben asegurar que sus operaciones se mantengan íntegras y protegidas frente a los riesgos inherentes al comercio nacional e internacional. En este contexto surge la certificación Business Alliance for Secure Commerce (por sus siglas en inglés, BASC), una iniciativa de alcance internacional, que promueve prácticas y estándares destinados a fortalecer la seguridad en empresas dedicadas a actividades de importación, exportación y servicios. Su propósito principal es reducir la posibilidad de que las operaciones sean utilizadas para fines ilícitos, entre ellos el contrabando, el terrorismo o el tráfico de drogas.

Si bien es cierto, esta herramienta inicia con un enfoque principalmente orientado a la protección integra de la cadena de suministros, no se centra únicamente en intervenir la parte operativa y logística, sino que lo hace en todos los niveles de la estructura organizacional, entendiendo que, cada uno de ellos es un eslabón que puede ser comprometido, lo que a su vez puede afectar a la cadena de suministros y a su vez a las operaciones normales de la empresa. Por lo tanto, en el estándar se presenta, para cada una de las áreas que componen la organización, controles que permiten reducir la probabilidad de que se presente un evento de seguridad.

Adicionalmente, una de las propuestas más importantes del estándar es promover la mejora continua en las instituciones que se adhieran a ella, recomendando que existan revisiones constantes de la conformidad de la empresa con su sistema de gestión y control de la seguridad y corregirlas, de forma oportuna, en caso de ser detectadas.

Más allá de ser un requisito competitivo para empresas que buscan operar en mercados globales, BASC se ha consolidado como una herramienta estratégica para generar confianza entre clientes, aliados comerciales y entidades reguladoras.

1.1 Antecedentes

Para este análisis, se propone como referencia una Empresa de Servicios Electrónicos, radicada en la ciudad de Cuenca y que mantiene operaciones en distintas regiones del país siendo sus puntos más fuertes Cuenca, Guayaquil y Quito, misma que se especializa en la comercialización al por mayor de dispositivos tecnológicos e informáticos, así como la prestación de servicios y soluciones tecnológicas corporativas. Su enfoque principal es el mercado nacional, pero la expansión de sus actividades y la naturaleza de sus productos, caracterizados por su alto valor tecnológico, la exponen a desafíos relacionados con la manipulación, almacenamiento y transporte de mercancía.

En el caso particular de las organizaciones dedicadas a servicios electrónicos —donde la gestión de información crítica y la interacción con cadenas logísticas son parte del día a día— la adopción del estándar adquiere un valor especial. Su implementación permite reducir vulnerabilidades, fortalecer los procesos internos y asegurar el cumplimiento de normativas relacionadas con la seguridad

Para la versión del estándar actualmente en vigencia, se incorpora, respecto a versiones anteriores, un apartado muy robusto de Seguridad de la Información, ya que considera, que la creciente influencia de la tecnología en las operaciones empresariales, no siempre van de la mano con las buenas prácticas y los controles, mismos que tienen la finalidad de crear una cultura del buen uso del equipamiento asignado a los usuarios y también, que permitan mantener la infraestructura tecnológica segura tanto a nivel físico como a nivel lógico.

Este estudio tiene como objetivo principal, evaluar la posición actual de la empresa de servicios electrónicos respecto a los requisitos de la certificación BASC, detectar posibles áreas de mejora y diseñar un plan de implementación acorde con sus operaciones. La integración de este modelo no solo contribuirá a minimizar la exposición a riesgos, sino que también fortalecerá la reputación institucional, optimizará los procesos de auditoría interna y permitirá una mejor adaptación a futuras regulaciones del mercado local.

Para dar por finalizado el proceso, el capítulo Azuay la organización World Basc Organization (por sus siglas en inglés, WBO), se encarga de realizar una auditoría general de todos los controles entregados por el estándar y emitir la certificación en base a las conformidades con su sistema de gestión

2 Determinación del Problema

En el contexto actual de seguridad en Ecuador, medios de comunicación han reportado un incremento significativo en delitos que afectan a las unidades económicas, principalmente en zonas urbanas con alta concentración comercial. Se presenta un creciente registro de robos a establecimientos comerciales, extorsiones y otros delitos violentos, así como un crecimiento en delitos informáticos, cuyo principal objetivo han sido empresas.

Este panorama ha generado un impacto negativo en la operatividad y estabilidad de las empresas, especialmente aquellas que manejan inventarios de alto valor y mantienen relaciones con diversos actores logísticos. Las provincias de Pichincha, Guayas y Azuay han sido algunas de las más afectadas por estos delitos, lo que ha llevado a las empresas a reforzar sus medidas de seguridad y evaluar estrategias para mitigar riesgos.

2.1 Descripción del problema

La creciente inseguridad en el medio en el cual se desenvuelve la Empresa de Servicios Electrónicos, sumado a la falta de una cultura organizacional adecuada, han conseguido que la imagen de la empresa haya sido afectada, por distintas causas que van desde retrasos en distribución, entregas de artículos erróneos, manejo inadecuado de la información de los usuarios de las organizaciones clientes, deficiente organización de inventario, insuficientes controles de acceso a las distintas zonas, etc. Todos estos problemas han derivado en la terminación de contratos y dificultad para mantener y encontrar nuevos socios comerciales.

2.2 Formulación del problema

La Empresa de Servicios Electrónicos que no cuenta con un estándar que le permita protegerse contra las diferentes amenazas, tanto internas como externas, requiere

una solución integral que permita proteger el normal funcionamiento de las operaciones de la organización, su información crítica y la de sus socios comerciales, implantando una cultura organizacional que se oriente a la seguridad en todos los niveles, mitigando los riesgos y generando así una ventaja competitiva basada en su imagen y confianza.

2.3 Delimitación del problema

Ante la falta de un marco de gestión de seguridad, se revisa el proceso implementación del estándar BASC en su versión 6 y se desarrolla el punto concerniente a Seguridad de la Información, sobre los cuales se delimitarán los siguientes aspectos:

- **Políticas y procedimientos:** Analizar las políticas y procedimientos internos implementados en la empresa.
- **Controles del estándar BASC:** Analizar los controles presentes en el estándar BASC V6 en el área de Seguridad de la Información.
- **No Conformidades:** Validar las no conformidades con el estándar BASC y proponer un proceso de remediación.
- **Mejora Continua:** Establecer un proceso de mejora continua que permita mantener el control de riesgos a través del tiempo.

2.4 Justificación del problema

La certificación BASC, se presenta como una herramienta esencial para reforzar la seguridad de forma integral a lo largo de toda la cadena de suministro. Implementar este estándar no solo contribuye a reducir los riesgos asociados al manejo, almacenamiento y transporte de mercancías, sino que también incrementa la competitividad y la reputación de la empresa en el mercado, demostrando su compromiso con las mejores prácticas de seguridad empresarial.

En concordancia con esto, la implementación de la certificación BASC representa una medida proactiva que se alinea con las exigencias del entorno empresarial

actual. Se trata de una valiosa herramienta que, no solo refuerza la cultura organizacional de seguridad, sino que también fomenta la mejora continua y protege la integridad de las operaciones frente a amenazas externas e internas, asegurando que todas las actividades de la empresa se realicen bajo condiciones óptimas de seguridad.

Para la Empresa de Servicios Electrónicos, adoptar los principios de seguridad BASC no solo permitiría proteger tanto los activos físicos, como los digitales de la empresa, sino que también fortalecer su imagen ante clientes institucionales, proveedores internacionales y organismos de control. Esta certificación permitiría a la empresa posicionarse como un referente de seguridad en la cadena de suministro, facilitando auditorías, acceso a nuevos mercados y la participación en procesos de licitación que exigen el cumplimiento con estándares internacionales.

3 OBJETIVOS

Se detallan, a continuación, los objetivos establecidos en la propuesta de implementación del estándar internacional BASC V6.

3.1 OBJETIVO GENERAL

Analizar los requisitos del sistema de gestión BASC (Business Alliance for Secure Commerce) en relación con la ciberseguridad y proponer su implementación en la empresa, con el fin de fortalecer la protección de la información digital en la cadena logística y garantizar el cumplimiento de estándares internacionales de seguridad informática y comercio seguro.

3.2 OBJETIVOS ESPECÍFICOS

1. Identificar los requisitos de ciberseguridad dentro del sistema de gestión BASC, analizando los controles, protocolos y estándares exigidos para garantizar la protección de la información en la cadena logística.
2. Evaluar el estado actual de la seguridad informática en la Empresa de Servicios Electrónicos, determinando vulnerabilidades y brechas en sus sistemas tecnológicos que puedan comprometer la integridad y confidencialidad de los datos relacionados con sus operaciones comerciales.
3. Diseñar un plan de implementación de ciberseguridad conforme a los estándares BASC, estableciendo estrategias de mitigación de riesgos, medidas de protección contra ataques cibernéticos y políticas de seguridad digital para fortalecer la cadena de suministro.
4. Capacitar al personal en buenas prácticas de ciberseguridad dentro del marco de la certificación BASC, promoviendo el uso adecuado de herramientas digitales, el manejo seguro de información y la concienciación sobre amenazas cibernéticas.

5. Evaluar la efectividad de las medidas de ciberseguridad implementadas, asegurando el cumplimiento de los estándares internacionales y la mejora continua de la protección de datos en la empresa.

4 Marco teórico referencial

En la actualidad, la ciberseguridad se ha convertido en una necesidad estratégica para las organizaciones, especialmente aquellas que forman parte de cadenas logísticas, comerciales y tecnológicas. El incremento de amenazas en este ámbito a nivel global, junto con la creciente dependencia de sistemas digitales para la gestión operativa, ha hecho que los riesgos asociados a la pérdida, alteración o robo de información sean cada vez más frecuentes y costosos. (Dal Cin & Jurgens, 2023)

En el caso de Ecuador, se ha evidenciado un aumento sostenido en los incidentes de seguridad informática, afectando tanto a instituciones públicas como a empresas privadas. Casos recientes de ataques a entidades gubernamentales, han demostrado la vulnerabilidad del país frente a amenazas digitales, y la necesidad urgente de adoptar buenas prácticas internacionales que garanticen la integridad de los sistemas y la continuidad del negocio. (ARCOTEL, 2024)(ARCOTEL, 2024) (ARCOTEL, 2024)

En este contexto, el presente proyecto tiene como finalidad analizar los requisitos del sistema de gestión BASC (Business Alliance for Secure Commerce) primero de forma general, para luego profundizar en lo que respecta a la seguridad de la información, que en su versión 6 incluye controles en seguridad de la información más fuertes, y proponer su implementación en una empresa de servicios electrónicos, con el propósito de fortalecer la protección de la información digital a lo largo de su cadena logística. El estándar BASC, ampliamente reconocido en el ámbito del comercio internacional, proporciona una base sólida para gestionar riesgos relacionados con la seguridad, incluyendo aquellos vinculados a la tecnología de la información. (World BASC Organization, n.d.)

Una empresa de servicios electrónicos dedicada a la comercialización y soporte tecnológico requiere implementar políticas y procedimientos que le permitan mejorar su posición frente a amenazas, reducir brechas en sus sistemas actuales y garantizar el cumplimiento de estándares internacionales. Este proyecto no solo

busca reducir vulnerabilidades técnicas, sino también fomentar una cultura organizacional en el ámbito de la seguridad de la información, en la que todos los actores de la empresa participen activamente en la protección de los activos digitales. (ISO/IEC, 2022a)(ISO/IEC, 2022a)(ISO/IEC, 2022a)

La propuesta contempla un enfoque integral: diagnóstico, implementación de medidas, capacitación del personal y evaluación continua. De este modo, se contribuye a la mejora de la competitividad empresarial, el cumplimiento de normativas internacionales y la reducción del riesgo operativo, en un entorno donde la información se ha convertido en uno de los activos más valiosos y vulnerables. (Bank & States, 2016)

4.1 Revisión de Requisitos de la Norma BASC

Cuando realizamos el control documental de la normativa vigente en la empresa, iniciamos el proceso de implementación del Sistema de Gestión en Control y Seguridad (por sus siglas, SGCS), mismo que está fundamentado en la conformidad de una serie de controles que deben ser debidamente registrados y probados, a los que se refieren como el estándar BASC.

Esta sección busca identificar y definir los requisitos establecidos por la norma BASC cuya finalidad es servir como base normativa y operativa desde la cual se deben construir las iniciativas de implementación posteriores. (World BASC Organization, 2022)

4.1.1 Contexto De La Empresa

Iniciamos el proceso revisando el contexto de la empresa, esto requiere analizar la parte organizacional, la estructura empresarial y las funciones que desempeña cada colaborador. La empresa, con la orientación mencionada, debe desarrollar y mantener un documento formal que describa cómo realizó el análisis de contexto, así como conocer los factores internos y externos que pueden influir en su sistema

de gestión BASC. Los factores identificados deben tener relación con el propósito de la empresa, la estrategia de negocio, y, sobre todo, los objetivos del SGCS BASC que va a ayudar a prevenir actos ilícitos, garantizar trazabilidad, o asegurar la integridad de la cadena logística (World BASC Organization, 2022)

El contexto de la empresa como tal, lo obtenemos con una matriz **FODA** (por sus siglas, Fortalezas Oportunidades Debilidades y Amenazas), que es una herramienta analítica y de carácter estratégico para identificar los factores internos y externos que inciden en su desempeño y competitividad de la organización. Usando esta metodología se evalúan las fortalezas y debilidades propias de la entidad, así como el reconocimiento de oportunidades y amenazas propias de su entorno, con esto, se pueden formular estrategias orientadas a mejorar sus capacidades internas, reducir vulnerabilidades, aprovechar condiciones favorables del mercado y mitigar los riesgos. Su aplicación es fundamental para la toma de decisiones, la planificación y adaptación en su entorno. (Dirección General De Desarrollo Institucional Y Aseguramiento De La Calidad, 2025)

Con el contexto también se identifican las partes interesadas y las organizamos en una **Matriz de Identificación de Partes Interesadas** que facilita a la entidad la comprensión de los miembros de su entorno, ya que considera variables como el nivel de interés, el grado de influencia, las expectativas y el tipo de vinculo que mantienen. Su finalidad es promover estrategias que permitan mejorar la colaboración con el fin de lograr los objetivos institucionales. (Restrepo-Olarte & Cogollo-Flórez, 2021)

A continuación, definimos el alcance, esto para delimitar como los procesos y actividades intervienen en la cadena logística y con ellos encontrar los riesgos operativos que presentamos en una **Matriz de Riesgos**. Con esta, identificamos y evaluamos los riesgos para priorizar aquellos que mayor afectación puedan tener en las operaciones de la empresa. (Consejo Profesional de Ciencias Económicas, 2023)

La norma promueve que la empresa tenga un enfoque de procesos, para esto es utilizamos un **Mapa de Procesos** en el que utilizamos los procesos y actividades que identificamos en el punto anterior, pero ilustrando las diferentes conexiones e interacciones dentro de las funciones de la organización. (World BASC Organization, 2022; World BASC Organization, 2022)

Para asegurar el cumplimiento del estándar, se estableció una **Política de Gestión y Control de Seguridad**, en la que se determinaron roles y responsabilidades específicas dentro de cada proceso. (Mamami et al., 2023)

4.1.2 Liderazgo

Este es uno de los puntos más críticos dentro de la implementación de cualquier certificación, ya que la Alta Gerencia debe asumir un compromiso firme con el proceso, gestionando oportunamente la documentación para mantener la conformidad, normativa y legal, y también, garantizar la disponibilidad de recursos que sean necesarios para el Sistema de Gestión de Control y Seguridad - BASC. (Méndez Morales & Yupa Cabadiana, 2019; World BASC Organization, 2022)

Otra parte de este compromiso es la revisión periódica de los objetivos estratégicos del sistema de gestión, de forma que estos se encuentren alineados con los objetivos institucionales.

Cada uno de los colaboradores de la empresa, deben tener claros sus roles y responsabilidades dentro del sistema de gestión, por lo que se tienen que documentar y formalizar la asignación tanto a los Representantes BASC quienes se encargan de dar seguimiento a su implementación continua, el encargado de seguridad, auditores internos de cada área.(BASC Ecuador Capítulo Cuenca, 2025; BASC Global, 2025)(BASC Ecuador Capítulo Cuenca, 2025; BASC Global, 2025)(BASC Ecuador Capítulo Cuenca, 2025; BASC Global, 2025)

4.1.3 Planificación

Como los recursos de las organizaciones son limitados, es necesario evaluar todos los riesgos que puedan afectar las actividades de la organización y priorizar aquellos

representen un mayor impacto. Con esto en consideración, implementamos una **Matriz de Evaluación de Riesgos**, en la que podemos evaluar cada uno de ellos considerando impacto y probabilidad de que ocurra.(Guerrero Aguiar et al., 2020)

Tomando esto como base, implementamos una **Matriz de Gestión de Riesgos**, en la que gráficamente, podemos clasificar los riesgos por nivel de criticidad, enfocando los esfuerzos a los más críticos.(International Organization for Standardization, 2018)

4.1.4 Apoyo

En este apartado, englobamos todos los recursos sobre los cuales se va a sostener el sistema de gestión. Para esto, identificamos los recursos humanos, materiales tecnológicos y financieros que se destinaron para garantizar que se dé el correcto desarrollo de todos los procesos y el cumplimiento normativo.

El control documental realizado para el **Sistema de Gestión de Previsiones** permite planificar y asignar los recursos adecuadamente, para eso se incluyen presupuestos detallados y revisión periódica del uso de los recursos, que, al ser aprobadas por la alta gerencia, permite que sea parte de las prioridades estratégicas empresariales. (Ó. E. Mora Navarro, 2022)

La gestión del personal establece que cada uno de los miembros de la empresa deben estar correctamente capacitados para el cumplimiento de sus funciones y su rol dentro de la organización, para lo cual se evalúan mediante una **Matriz de Cargos Críticos.** Para asegurar que la formación del personal se la adecuada, se planificó un programa de **Entrenamiento y Capacitación**. (Mantilla Rivera, 2024)

4.1.5 Evaluación de desempeño

La gerencia debe garantizar la eficacia del sistema de gestión, para lo cual se planteó un **Plan de Auditorías Internas**, con la finalidad de verificar la conformidad, evaluar la eficacia y detectar oportunidades de mejora.(Consejo Nacional de Evaluación de la Política de Desarrollo Social, 2025)

4.1.6 Mejora

El proceso de auditoría implementado da como resultados hallazgos en los cuales se observa el nivel de conformidad, observaciones u oportunidades de mejora. (O. E. Mora Navarro, 2022)

Los hallazgos permiten priorizar actividades que tienen mayor impacto para intervenirlas inmediatamente con planes de acción específicos determinando responsables, plazos y recursos necesarios para dar cumplimiento.(Salgado Romero, 2025)

4.2 BASC V6 en Seguridad de la Información

En el estándar BASC, se establecen los controles que se orientan a la protección de la infraestructura tecnológica, compuesta por servidores, equipos de red, dispositivos de usuario final, etc, ya que constituyen un activo estratégico dentro de la organización y que debe ser protegida en todas sus fases, garantizando así la confidencialidad, integridad y disponibilidad de los datos.(World BASC Organization, 2022)

4.2.1 Controles para Seguridad de la Información

Del estudio efectuado se extrajo el listado con los controles en el apartado Seguridad de la Información que, según el estándar BASC, debe cumplir la empresa para fortalecer la seguridad en sus actividades. La validación de estos controles permitió verificar el estado inicial de la empresa realizando una evaluación de la estructura operativa interna de la organización.(WBO, 2022)(WBO, 2022)(WBO, 2022)

4.2.1.1 Generalidades

a) Gestionar y proteger el manejo de la información y los recursos informáticos de la empresa, incluyendo las medidas a aplicar en caso de incumplimiento.

La empresa debe establecer controles para proteger los activos tecnológicos, que deben estar custodiados por un miembro de la organización, que es el responsable de su buen uso y se determina también mecanismos en caso de incumplimientos.(ISO/IEC, 2022b; Mamami et al., 2023)(ISO/IEC, 2022b; Mamami et al., 2023)(ISO/IEC, 2022b; Mamami et al., 2023)

b) *Salvaguardar la información y su confidencialidad, integridad y disponibilidad, en sus diferentes formas y estados.*

La empresa debe garantizar la seguridad de su información en todas sus formas, para esto debe mantener la información disponible, inalterable y con accesos controlados. (UDAX, 2024)(UDAX, 2024)(UDAX, 2024)

c) *Proteger la infraestructura de las tecnologías de la información*

La empresa debe implementar medidas para resguardar, todos los componentes físicos y lógicos que la componen, de cualquier amenaza que puedan comprometer su funcionalidad.(ISO/IEC, 2022b)(ISO/IEC, 2022b)(ISO/IEC, 2022b)

4.2.1.2 Ciberseguridad y las tecnologías de la información

a) *Establecer, documentar y mantener criterios de seguridad que permitan identificar y proteger los sistemas de las tecnologías de la información y recuperarla oportunamente en caso de ser necesario*

Se deben establecer criterios de seguridad mediante políticas enfocadas en salvaguardar y definir planes de contingencias en caso de presentarse un evento que lo requiera. (Mamami et al., 2023)(Mamami et al., 2023)(Mamami et al., 2023)(Mamami et al., 2023)

b) *Identificar partes interesadas y su nivel de criticidad en la infraestructura informática (hardware y software) de la empresa.*

Se deben definir medidas que permitan una correcta categorización basada en la criticidad del cargo y las funciones que realiza.(Khadka & Ullah, 2025)(Khadka & Ullah, 2025)(Khadka & Ullah, 2025)(Khadka & Ullah, 2025)

c) *Comunicar oportunamente información sobre amenazas de ciberseguridad identificadas a las partes interesadas correspondientes.*

Es necesario establecer los canales formales de comunicación para que la información, referente a amenazas, fluya hacia eficazmente y permita una respuesta oportuna.(Cremer et al., 2022)(Cremer et al., 2022)(Cremer et al., 2022)(Cremer et al., 2022)

d) *Clasificar la información de acuerdo con la legislación vigente, sistemas y accesos según el nivel de criticidad y establecer políticas de acceso a la misma.*

En el ecuador, se debe garantizar el cumplimiento de la Ley Orgánica de Protección de Datos Personales (por sus siglas, LOPDP) y como complemento el uso del principio de mínimo privilegio en la norma ISO/IEC 27001:2022.(IEEE Communications Society, n.d.; ISO/IEC, 2022b; LOPDP, 2021)(IEEE Communications Society, n.d.; ISO/IEC, 2022b; LOPDP, 2021)(IEEE Communications Society, n.d.; ISO/IEC, 2022b; LOPDP, 2021)(IEEE Communications Society, n.d.; ISO/IEC, 2022b; LOPDP, 2021)

e) *Utilizar cuentas asignadas para cada usuario que acceda al sistema, con sus propias credenciales de acceso mediante contraseñas u otras formas de autenticación que generen accesos seguros. Estas deben actualizarse periódicamente, cuando existan indicios o sospechas razonables de que están comprometidas.*

Se debe establecer que las credenciales de acceso son de uso personal y no deben ser compartidas, complementando con la ISO/IEC 27001:2022 que establece la gestión segura del ciclo de vida de las credenciales.(ISO/IEC, 2022a; Sargiotis, 2024)

f) *Limitar los accesos y permisos de los usuarios de acuerdo con las funciones y tareas asignadas, revisándolos periódicamente.*

Según la categorización de la información, limitar los accesos siguiendo el principio de mínimos privilegios mediante políticas de control de acceso basado en roles. (ISO/IEC, 2022a; Sargiotis, 2024)

g) *Eliminar el acceso a la información a todos los colaboradores, terceros y usuarios externos al terminar su contrato o acuerdo.*

La revocación de accesos al finalizar contratos o relaciones laborales evita que excolaboradores o terceros mantengan privilegios que puedan generar riesgos de seguridad.(ISO/IEC, 2022a; Sargiotis, 2024)(ISO/IEC, 2022a; Sargiotis, 2024)

h) *Impedir la instalación de software no autorizado.*

Se define mediante políticas que solo el personal autorizado, cuenta con los permisos para esta función.(ISO/IEC, 2022b; Sargiotis, 2024)(ISO/IEC, 2022b; Sargiotis, 2024)

i) *Utilizar y mantener hardware y software licenciados y actualizados para proteger la infraestructura de TI contra amenazas informáticas tales como virus, programas espías, gusanos, troyanos, malware, ransomware, entre otros.*

Las puertas traseras que se presentan en muchas organizaciones, es el uso de software sin licencia o activado mediante cracks y la falta de actualizaciones en el software de la empresa.(ISO/IEC, 2022a; Sargiotis, 2024)(ISO/IEC, 2022a; Sargiotis, 2024)

j) *Realizar copias de seguridad de la información sensible, manteniendo un respaldo fuera de las instalaciones (física o virtual) con las medidas de seguridad necesarias para impedir que terceros accedan a la información.*

Se debe respaldar la información cifrada y en medios con los niveles de acceso más elevados dentro de la organización, mismos que se planifican de acuerdo con el nivel de criticidad de cada activo de información. (ISO/IEC, 2022a; Sargiotis, 2024)(ISO/IEC, 2022a; Sargiotis, 2024)

k) *Mantener un registro actualizado de los usuarios, su nivel de criticidad y accesos asignados.*

La administración de identidades y accesos (IAM), que con la norma ISO/IEC 27001:2022 (control A.5.17) automatizan la gestión y trazabilidad de accesos integrando datos de distintas plataformas, lo que facilita auditorías, detección de anomalías y el cumplimiento normativo. (Cremer et al., 2022; ISO/IEC, 2022b)(Cremer et al., 2022; ISO/IEC, 2022b)

l) *Cerrar/bloquear la sesión en equipos desatendidos.*

Dejar equipos de cómputo desatendidos sin cerrar o bloquear la sesión aumenta el riesgo de accesos indebidos y manipulaciones maliciosas. La norma ISO/IEC 27001:2022 (control A.5.20) exige que los usuarios cierren sesión o activen el bloqueo automático cuando los dispositivos no estén en uso, como parte de la defensa en profundidad. (ISO/IEC, 2022b; Mamami et al., 2023)(ISO/IEC, 2022b; Mamami et al., 2023)

m) *Evaluar mínimo una vez al año la seguridad de la infraestructura de TI (hardware y software), implementando acciones pertinentes cuando se hayan detectado vulnerabilidades.*

Las organizaciones deben evaluar de forma periódica la seguridad de su infraestructura de TI para identificar vulnerabilidades, errores de configuración y riesgos que afecten la confidencialidad, integridad y disponibilidad de sus activos. La norma ISO/IEC 27001:2022 (control A.5.36) exige revisar la eficacia de los controles mediante pruebas como pentesting, análisis de vulnerabilidades y auditorías. (ISO/IEC, 2022c, 2022b)(ISO/IEC, 2022c, 2022b)

n) *Establecer procedimientos y controles para identificar y revisar el acceso no autorizado a los sistemas de información, sitios web, o el incumplimiento de las políticas y procedimientos (incluyendo la manipulación o alteración de los datos comerciales por parte de los colaboradores o contratistas).*

Tomando como referencia la norma ISO/IEC 27001:2022 control (A.5.23) que utiliza registros detallados, protegidos y regularmente inspeccionados para garantizar la trazabilidad y hacer más fácil la revisión de incidentes en Sistemas de información, páginas web que están expuestos a accesos indebidos o manipulación de datos. (ISO/IEC, 2022a, 2022c)(ISO/IEC, 2022a, 2022c)

o) *Revisar las políticas y los procedimientos de ciberseguridad al menos una vez al año, y actualizarlas cuando se presenten cambios en el contexto interno o externo, o cuando se materialice algún riesgo.*

La evaluación periódica de la conformidad con los controles permite mantener la eficacia del sistema de gestión. Según la norma ISO/IEC 27001:2022 en su control A.5.1 este proceso se lo debe planificar cada determinado tiempo o cuando exista un cambio importante. (ISO/IEC, 2022a)(ISO/IEC, 2022a)

p) *Emplear tecnologías seguras, como redes privadas virtuales (VPN) o autenticación multifactor para el acceso seguro de los colaboradores y usuarios externos a los sistemas informáticos de la empresa, incluyendo accesos para trabajo remoto o teletrabajo*

Lo mecanismos de autenticación empleados se encuentran determinados en la norma ISO/IEC 27001:2022 y se relacionan directamente con el nivel de criticidad del recurso al que se tiene que acceder. En los niveles más críticos se recomienda el uso combinado de multifactor con VPN. (ISO/IEC, 2022a, 2022c)(ISO/IEC, 2022a, 2022c)

q) *Establecer procedimientos para evitar el acceso remoto de usuarios no autorizados, desde dispositivos personales u otros*

En el control A.5.19 de la ISO/IEC 27001:2022 determina que el acceso remoto a sistemas internos de la empresa representa un riesgo si no se toman medidas adecuadas como complementarlos con autenticación de multifactor y registrando los equipos que se pueden ingresar a ellos. (ISO/IEC, 2022a; Sargiotis, 2024)(ISO/IEC, 2022a; Sargiotis, 2024)

r) *Controlar mediante la realización de inventarios periódicos, los medios u otros equipos que hagan parte de la infraestructura informática de la empresa. La eliminación o desecho de los mismos se hará de acuerdo con la legislación vigente.*

La realización de inventarios periódicos a los activos informáticos para registrar su estado tomando la recomendación de la norma ISO/IEC 27001:2022 que indica que se debemos llevar el control durante todo el ciclo de vida del activo. (ISO/IEC, 2022c, 2022a; Sargiotis, 2024)(ISO/IEC, 2022c, 2022a; Sargiotis, 2024)

s) *Restringir la conexión de dispositivos personales y elementos periféricos no autorizados para cualquier dispositivo que forme parte de la infraestructura informática de la empresa.*

Se debe restringir el uso de dispositivos externos como se recomienda en el control A.5.10 de la norma ISO/IEC 27001:2022 en donde incluyen desactivación de los puertos de los usuarios e implantación de listas blancas con dispositivos permitidos. (CNCS, 2020; ISO/IEC, 2022a)(CNCS, 2020; ISO/IEC, 2022a)

t) *Vigilar el cumplimiento de las políticas de ciberseguridad y seguridad de la información establecidas en el uso de plataformas y contenido digital, herramientas de videoconferencia, comercio electrónico, entre otras.*

El cumplimiento de las políticas es fundamental, por lo que se debe establecer un plan de auditoría que verifique lo establecido, o a su vez emplear herramientas de monitoreo, esto se describe en la norma ISO/IEC 27001:2022 con su controL A.5.35. (ENISA, 2021; ISO/IEC, 2022a)(ENISA, 2021; ISO/IEC, 2022a)

u) *Realizar ejercicios prácticos y/o simulacros relacionados con la seguridad de las tecnologías de la información, que permitan determinar la eficacia de las acciones establecidas (ver Norma 6.1 e).*

La constante evolución de las amenazas informáticas obliga a realizar pruebas de políticas y controles para evaluar su efectividad y registrar hallazgos y actualizarlos con el uso de la norma ISO/IEC 27001:2022 en el control A.5.36. (ENISA, 2021; ISO/IEC, 2022a)

v) *Establecer controles para super usuarios que permitan la continuidad de credenciales de los equipos activos, en caso que aplique.*

Dado que lo super usuarios mantienen permisos con privilegios elevados, también requiere controles más estrictos como lo establece en su control A.5.18 la norma ISO/IEC 27001:2022. (ISO/IEC, 2022b, 2022c)

Una vez definido el marco normativo, se analiza la infraestructura de la empresa y el nivel de cumplimiento.

5 Análisis de la Conformidad de la empresa con el Estándar BASC

Como requisito previo, el estándar BASC V6 en seguridad de la Información exige la realizar un diagnóstico completo del entorno tecnológico actual de la organización, cuyo objetivo es evaluar la infraestructura informática, identificando vulnerabilidades, prácticas inadecuadas y brechas que comprometen la protección de los datos. Esta evaluación constituye la base para priorizar acciones de mitigación y definir estrategias de seguridad sostenibles y eficaces, orientadas a reducir riesgos y garantizar la integridad de la información.(BASC Global, 2025; Méndez Morales & Yupa Cabadiana, 2019)

En cuanto a las operaciones de la empresa en estudio, sus actividades se desarrollan en dos líneas de negocios:

La primera se centra en la comercialización y arrendamiento de equipos tecnológicos, lo que sustenta la segunda línea. la prestación de servicios asociados al arrendamiento.

Estos servicios incluyen una mesa de ayuda, la gestión y administración del servicio de impresión, la generación y administración de respaldos de información, así como otras soluciones orientadas a optimizar la operación tecnológica de los clientes. Esta combinación permite ofrecer un portafolio integral que asegura continuidad, eficiencia y soporte especializado.

5.1 Análisis organizacional del área de TI

La empresa asigna dos colaboradores en calidad de para el área de TI que cumplen con las funciones de: administrar, dar soporte tecnológico, y, además, comparten la responsabilidad de gestionar la infraestructura interna.

El primer colaborador es el Desarrollador, tiene a su cargo el desarrollo de nuevas funcionalidades y mejoras dentro del Sistema de Inventarios, y también, la administración y el soporte al ERP.

El segundo colaborador, Analista TI, es responsable de la administración y el soporte de la infraestructura física de la organización, además, gestiona aplicaciones y realiza respaldos de información tanto de usuarios como de sistemas, asegurando la continuidad operativa y la protección de los datos.

5.2 Infraestructura Tecnológica Inicial

Se inició con una revisión física, considerando el entorno y las condiciones que influyen en la seguridad de los recursos tecnológicos. Luego, se procede a identificar y enumerar los componentes de la infraestructura tecnológica, incluyendo servidores, equipos de red, dispositivos de almacenamiento y demás elementos críticos para la prestación de servicios. Finalmente, se realiza un inventario y evaluación de las aplicaciones implementadas, verificando su funcionalidad, nivel de actualización y grado de alineación con los requisitos del Sistema de Gestión de Seguridad BASC.

5.2.1 Distribución de las instalaciones de la Empresa de Servicios Electrónicos

La empresa desarrolla sus actividades en instalaciones compartidas con otras compañías y usuarios, distribuidas en tres niveles.

En el primer piso ocupa la totalidad del espacio, organizado en cinco secciones: dos destinadas al área comercial, una para la bodega principal y las dos restantes para el departamento técnico.

El segundo piso cuenta con cuatro secciones, de las cuales la empresa utiliza dos: una para el área administrativa y otra para una segunda bodega.

Finalmente, en el tercer piso se dispone de una sección adicional que funciona como tercera bodega.

El centro de la infraestructura tecnológica, que incluye el core de la red y el conjunto de servidores, se encuentra ubicado dentro del espacio asignado al departamento técnico. Esta área posee una única entrada que conduce a una recepción destinada a la atención de clientes.

Tras la recepción, se accede a un pasillo que conecta con la sala de trabajo del equipo técnico, esta es una sala de un solo ambiente, sin divisiones, donde se realizan tareas de mantenimiento y reparación de equipos de cómputo e impresoras, tanto para usuarios bajo contrato de alquiler como para clientes externos.

En esta misma sala se encuentra el rack en el que se encuentran los equipos físicos, se trata de un armario de 36 UR, equipado con puertas delantera y posterior; la puerta trasera permanece abierta para facilitar la ventilación y el acceso, mientras que la delantera se mantiene cerrada, aunque sin utilizar la cerradura.

5.2.2 Inventario del centro de Infraestructura Tecnológica

Dentro del núcleo de la infraestructura tecnológica, responsable de gestionar los servicios internos y la comunicación corporativa, se encuentra el core de la red. Este núcleo está conformado por un router identificado como R1 y un firewall denominado F1, ambos provistos y administrados por la empresa que suministra el servicio de internet. El firewall opera en modo switch, y desde sus puertos se establece la conexión hacia tres switches administrables Cisco, identificados como SW1, SW2 y SW3, cuya función principal es interconectar las distintas áreas de la empresa y garantizar la comunicación con el grupo de servidores.

El grupo de servidores está compuesto por tres equipos físicos. Dos de ellos, denominados SRV1 y SRV2, funcionan como contenedores sobre los cuales se implementan servidores virtuales que soportan diversos servicios internos. El tercer servidor, identificado como SRV3, cumple la función de almacenamiento centralizado, proporcionando recursos de almacenamiento para los servidores virtuales alojados en SRV1 y adicionalmente, un equipo que cumple con las

funciones de NAS. Esta arquitectura permite una distribución eficiente de cargas de trabajo y asegura la escalabilidad de los servicios tecnológicos.

5.2.3 Inventario del Ecosistema de Infraestructura de Software Empresarial

Para garantizar el funcionamiento normal de la empresa, se realiza un control periódico de los servicios activos y del personal responsable de su administración. A continuación, se detalla la infraestructura lógica y los sistemas implementados:

Servidor A/D (Directorio Activo, por sus siglas en inglés Active Directory), se encuentra virtualizado en SRV1, permite la administración de usuarios y despliegue de políticas dentro del dominio empresarial que se encuentra habilitado en este mismo servidor DNS (Servidor de dominio de red, por sus siglas en inglés Domain Network Services), permitiendo la resolución de nombres de dominio, y, además, mantiene activo WSUS (Servidor para el Servicio de Actualizaciones de Windos, de sus siglas en inglés Windows Server Update Services) que entrega actualizaciones de sistema operativo Windows a los equipos registrados en AD. Se encuentra bajo responsabilidad del colaborador TI.

Servidor A/D 2 se encuentra virtualizado en SRV1, actúa como copia del AD principal y cumple funciones de respaldo para garantizar la continuidad del servicio en caso de fallos. Se encuentra bajo responsabilidad del colaborador TI.

Sistema de inventario se encuentra virtualizado en SRV2 que permite llevar el control de todos los activos y movimientos de inventario que ha mantenido la empresa, mismo que se encuentra en constante desarrollo para que su funcionalidad se adapte a las necesidades que tiene la empresa. Se encuentra bajo responsabilidad del colaborador Desarrollador.

Servidor de Desarrollo se encuentra virtualizado en SRV2, es un servidor que se mantiene activo con una imagen espejo del Sistema de Inventario para pruebas de los nuevos desarrollos antes de ser implementados en producción. Se encuentra bajo responsabilidad del colaborador Desarrollador.

Servidor de Base de datos, se encuentra virtualizado en SRV1, es un servidor en el que se almacenan las bases de datos del sistema de inventario, Se encuentra bajo responsabilidad del colaborador Desarrollador.

Servidor de respaldos, se encuentra virtualizado en SRV1, mantiene el servicio que permite realizar respaldos de los servidores que se encuentran instalados con un agente que provee el software. Este servicio es licenciado de paga, pero, en este caso, se utiliza una licencia de prueba con un vencimiento mensual, cargando cada mes una licencia gratuita de prueba nueva activando la versión limitada del software. Se encuentra bajo responsabilidad del colaborador TI.

Sistema ERP se encuentra virtualizado en SRV1, en el que se registran todos los movimientos contables, proformas y facturación a clientes, pagos de nóminas a los empleados, pagos a proveedores, etc. Se encuentra bajo responsabilidad del colaborador Desarrollador.

Servicio de Gestión de Impresión, se encuentra virtualizado en SRV1, es un sistema que permite gestión de usuarios, control de acceso, seguimiento a impresión, copias y escaneo para reportería. Se encuentra bajo responsabilidad del colaborador TI.

Antivirus se encuentra virtualizado en SRV1, es un antivirus empresarial con una consola que permite monitorear, visualizar eventos de seguridad de acuerdo con niveles de criticidad y gestionar políticas para control en los equipos que tengan instalado el agente antivirus y enlazado al servidor principal. Se encuentra bajo responsabilidad del colaborador TI.

Servicio de Monitoreo de Activos, se encuentra virtualizado en SRV1, es un instrumento que permite monitorear todos los equipos de computo que se encuentren conectados a la red empresarial y que mantenga instalado el agente de monitoreo. Este software identifica la serie del equipo y extrae de este el usuario que se encuentra activo, las características del equipo, software instalado en cada equipo. Se encuentra bajo responsabilidad del colaborador TI.

Mesa de Ayuda Interna virtualizado en SRV1, está destinado para incidentes tanto del público en general como las que se generen internamente al departamento técnico y TI, esta mesa de ayuda con licenciamiento de software libre, en la que se puede generar tickets para atención oportuna y seguimiento a los tiempos de solución, de forma que se obtiene actividades que realiza cada uno de los miembros del personal técnico. Se encuentra bajo responsabilidad del colaborador TI.

Mesa de Ayuda Clientes virtualizado en SRV1, es destinada para clientes de arrendamiento de equipos, de cómputo e impresión y tiene un licenciamiento de pago anual, que permite dar seguimiento de las solicitudes que se realicen al área operativa, como los incidentes que se redirijan al área técnica. Esta mesa de ayuda está limitada por el número de licencias, considerando que cada técnico que mantenga habilitado el inicio de sesión consume una licencia. Se encuentra bajo responsabilidad del colaborador TI.

NAS (Almacenamiento conectado a la red, por sus siglas en inglés Network Attached Storage), es un servidor montado sobre un equipo físico que cumple con la función de almacenar información valiosa de la empresa, entre ellas políticas y procesos aprobados, respaldos de correos y equipos de personal que sale de la empresa, etc. Se encuentra bajo responsabilidad del colaborador TI.

Sistema Monitoreo de Parque de Impresión, este es un sistema en la nube con licenciamiento mensual y es parte servicio de arrendamiento de impresoras, parte del servicio incluye el monitoreo y despacho de los suministros, por lo que, para cada impresora instalada en la infraestructura del cliente, se tiene también instalado un agente de monitoreo en el equipo del usuario, que cumple con la función de comunicarse con la impresora y extraer la información de niveles de suministros, niveles de consumibles, contadores de impresión, escaneo y copias. Se encuentra bajo responsabilidad del colaborador TI.

Aplicaciones Ofimáticas. Para que cada uno de los colaboradores puedan cumplir con sus funciones diarias, se le asigna una licencia de Microsoft 365, misma que contiene el listado completo de aplicaciones de office, correo electrónico con

Exchange Administrable, almacenamiento de información en la nube con OneDrive y gestor documental en la nube con SharePoint. Se encuentra bajo responsabilidad del colaborador TI.

5.3 Verificación de la conformidad de los Controles BASC V06:2022 en Seguridad de la Información

Se procede a levantar información sobre el estado actual de la empresa que incluye la recopilación de políticas internas, procedimientos operativos, registros de actividades, evidencias documentales y cualquier otro elemento que permita demostrar la implementación de controles relacionados con la seguridad de la información. También, se realizaron entrevistas con el personal responsable del área TI, Departamento Técnico y Talento Humano. (Méndez Morales & Yupa Cabadiana, 2019; World BASC Organization, 2022)

Se hicieron observaciones directas al cumplimiento de políticas y se validó la infraestructura física y tecnológica, asegurando que los datos obtenidos reflejen la realidad operativa.

Luego, se hizo el análisis comparativo entre los controles que exige el estándar BASC y las prácticas de la empresa. Este análisis permitió identificar brechas de cumplimiento, áreas críticas y oportunidades de mejora. El resultado de esta comparación permitió la elaboración del SGCS-BASC, en donde se detalla la conformidad de los controles en el estándar.

Este proceso no solo garantiza la transparencia y objetividad en la auditoría, sino que también proporciona a la organización una visión clara de su nivel de preparación frente a los requisitos BASC.

Dentro del proceso de auditoría para la certificación BASC, resulta indispensable no solo realizar la comparación entre los controles exigidos por el estándar y el estado actual de la empresa, sino también identificar, registrar y documentar los

instrumentos que respaldan cada uno de dichos controles. Este procedimiento tiene como finalidad establecer una trazabilidad clara entre los requisitos normativos y la evidencia documental que demuestra su cumplimiento. Para ello, se debe determinar con precisión en qué documentos se encuentran registradas las políticas, procedimientos y mecanismos que garantizan la conformidad con el estándar, asegurando que cada control esté debidamente soportado.

Si se determina que no existe evidencia suficiente o el documento actual no contemple el control requerido, se coloca la observación de que requiere modificación o actualización.

Este análisis es un elemento crítico para este proceso, ya que ayuda en la identificación de brechas y la planificación de mejoras, y, asegura que la empresa cuente con un sistema de gestión alineado a los principios BASC.

Además, este registro sistemático permite que la auditoría se desarrolle con transparencia y que la organización disponga de una base sólida para la implementación de controles preventivos y correctivos.

Control 6.1 a, referente a los controles y medidas de seguridad de la información se encuentran presentes en la Política de Seguridad TI.

Control 6.1 b, tiene como función limitar el acceso a la información clasificándola de acuerdo con su nivel de criticidad y al impacto que puede tener su perdida, esto se encuentra documentado en la Matriz de Criticidad.

Control 6.1 c, si bien el datacenter no se encuentra en un punto de acceso público, es accesible para todo el personal del departamento técnico y no existe una políticas para proteger el los activos.

Control 6.2 a, no existe documentado dentro de las políticas o procesos para la activación de los planes de contingencia para la recuperación en casos de eventos de seguridad.

Control 6.2 b, relacionado con los accesos a la información, es necesario identificar las partes interesadas, definir el nivel de criticidad que tienen dentro de la empresa, se encuentra documentado en la Política de Seguridad.

Control 6.2 c, se deben establecer los canales de comunicación pertinentes con las partes interesadas, de forma que la información referente amenazas de ciberseguridad fluya oportunamente y una vez definido, se debe documentar en la Política de Seguridad.

Control 6.2 d, la clasificación de la información no se encuentra alineada con la legislación actual vigente, por lo que este punto debe ser revisado y actualizado e incluirse dentro de la documentación.

Control 6.2 e, se encuentra establecido como recomendación de en las buenas prácticas y en políticas de TI, con el afán de ahorrar costos en licencias de aplicaciones, se hace uso de usuarios y cuentas compartidas en ciertas aplicaciones. Esto se debe documentar.

Control 6.2 f, una vez clasificada la información por su nivel de criticidad, es necesario clasificar a los colaboradores de acuerdo con el cargo que ocupan y las funciones que realizan, esto permite determinar a qué información pueden acceder, esto debe ser documentado.

Control 6.2 g, cada salida de personal o terminación de contrato, según la política de Salida de Personal, se deben realizar respaldos de la información contenida en el equipo que se entrega al usuario y boquear todos los accesos a las cuentas de los diferentes sistemas. Este proceso se lo documenta por cada usuario en un Informe de Retiro de Accesos.

Control 6.2 h, el software instalado en cada equipo de usuario de la empresa, debe ser supervisado y controlado por el Analista TI por lo que se monitorea diariamente mediane el Software de Monitoreo de Activos e identifica el listado de software instalado en los equipos. Esto se encuentra documentado en la Matriz de Seguridad TI.

Control 6.2 i, todo el software que se instale en la empresa, debe contar con licenciamiento para cada usuario, evitando así el uso de cracks que se conviertan en amenazas a la seguridad de la empresa, por lo que se debe desarrollar la documentación pertinente

Control 6.2 j, una de las aplicaciones del paquete Microsoft 365 es OneDrive que realiza respaldos de la información de los equipos de todos los usuarios en la nube y se almacenan periódicamente en Sharepoint, y para los servidores, se mantiene un servidor para respaldos diarios de todo el VCenter de la empresa.

Control 6.2 k, se mantiene actualizado el Listado de usuarios para mantener el registro de usuarios y accesos.

Control 6.2 l, dentro de la Política de Seguridad se mantiene registrado el bloqueo de la sesión del usuario activo en equipos desatendidos, ya que el estándar no recomienda un tiempo, se consideró la recomendación de la ISO 27000 que recomienda entre 3 a 5 minutos.

Control 6.2 m, en la Política de Seguridad se establece la evaluación de la infraestructura tecnológica de forma anual.

Control 6.2 n, la documentación digital de la empresa se la almacena en el entorno de Microsoft 365, desde los usuarios en OneDrive y el Gestor documental de la empresa en Sharepoint, estas dos herramientas mantienen activos los controles de autenticación y registros, pero también, su acceso está restringido únicamente para personal con una cuenta de la empresa, esto se encuentra documentado en la Política de Seguridad.

Control 6.2 o, en la Política de Seguridad se establece que anualmente se realiza la revisión de las políticas y procedimientos de la empresa, lo que incluye las políticas de Seguridad de la información.

Control 6.2 p, para el acceso desde fuera de la empresa hacia los sistemas internos, se entregan credenciales de VPN para acceder a través del firewall. Se habilita la

autenticación multifactor para todos los sistemas que tienen esta opción, se encuentra autorizado el uso en la empresa de Microsoft Authenticator.

Control 6.2 q, Analsita TI mantiene el registro de los usuarios que tienen autorización de alta gerencia para el acceso remoto y se establece en la Política de Seguridad que se restringe acceso remoto para todos los usuarios.

Control 6.2 r, no existe un proceso o política implantado para la eliminación de los acticos tecnológicos de la empresa, tampoco se realizan inventarios de estos activos desplegados.

Control 6.2 s, no existe control de dispositivos autorizados para acceder a la infraestructura empresarial o a los sistemas activos, esto por darle facilidad de conexión y comunicación a los colaboradores de la empresa.

Control 6.2 t, se establece realizar autorías periódicas a toda la infraestructura tecnológica de la empresa, para lo cual se detalla un plan de auditoría esto se encuentra correctamente documentado en la Política de Seguridad empresarial.

Control 6.2 u, dentro de la documentación se debe establecer un plan de simulacros de ataques en los distintos sistemas empresariales, de esta forma se pueda conocer claramente cuál sería el accionar del personal responsable y las partes interesadas.

Control 6.2 v, se debe registrar una política que permita el control al super usuario, en el caso de la empresa de servicios electrónicos, y en consideración que, la gestión de los sistemas de la empresa se encuentra dividida entre los dos miembros del área de TI quienes se encuentran catalogados como super usuarios y es a los dos a quienes se debe establecer los controles.

5.4 Evaluación del estado inicial de la Empresa

La evaluación de la infraestructura de la empresa, se lo representó mediante una matriz de control, que permita evidenciar de forma clara y concisa el cumplimiento de la empresa con los controles del estándar.

Esta matriz de control se alinea con los objetivos de la norma BASC, realizando un Sistema de Gestión de Control y Seguridad para cada una de las áreas, esto permite identificar, evaluar y verificar el cumplimiento de los controles, en el caso de Seguridad de la Información, relacionados con la gestión y protección de la información tecnológica y digital de la organización. Los parámetros representan los controles específicos, agrupados en los apartados 6.1 (Gestión de la información) y 6.2 (Ciberseguridad y tecnologías de la información).

En la matriz se detalló el responsable de cada control, el proceso al que pertenece, el estado actual de cumplimiento, la clase y las anotaciones que registran en la documentación o evidencia, de esta forma, se puede visualizar de manera completa el grado de cumplimiento de los requisitos de seguridad. Los controles que fueron marcados como “No” representan controles pendientes de implementación que deben mitigarse mediante planes de acción correctivos.

En conjunto, la matriz constituye una herramienta de diagnóstico, seguimiento y mejora continua que respalda el cumplimiento de los lineamientos BASC en materia de ciberseguridad y gestión de la información. Si bien es cierto, para este análisis, se aborda únicamente el apartado de Ciberseguridad y Tecnologías de la información, este análisis se aplica en todos los apartados de la normativa, evaluando su cumplimiento.

Finalmente, la matriz en Tabla 1 presenta el porcentaje de cumplimiento en el que la empresa se encuentra actualmente, siendo un indicador base, para determinar el estado inicial de la empresa y los avances que se puedan lograr. Como evaluación preliminar, la empresa cumple únicamente con el 60% de los controles solicitados

por el estándar, que, si bien se tiene una buena base de partida, es insuficiente, de cara a una Auditoría de Certificación.

Tabla 1. Matriz de Control del SGCS-BASC de la Empresa de Servicios Electrónicos

REQ.	PARAMETROS	RESPONSABLE	PROCESO	ESTADO	ANOTACIONES
6	SEGURIDAD DE LA INFORMACIÓN				
6,1	Generalidades				Procedimiento de Seguridad TI
6.1 a	Gestionar y proteger información y tecnología	Analista TI	Seguridad TI	Si	Política de Seguridad de TI
6.1 b	Salvaguardar información confidencial	Analista TI	Seguridad TI	Si	Matriz de Criticidad
6.1 c	Proteger infraestructura tecnológica	Analista TI	Seguridad TI	No	
6,2	Ciberseguridad y las tecnologías de información				
6.2 a	Criterios de seguridad (Proteger y recuperar)	Analista TI	Seguridad TI	No	
6.2 b	Identificar partes interesadas	Analista TI	Seguridad TI	Si	Política de Seguridad
6.2 c	Comunicar amenazas de ciberseguridad	Analista TI	Seguridad TI	Si	Política de Seguridad
6.2 d	Clasificar información según criticidad	Analista TI	Seguridad TI	No	
6.2 e	Cuentas asignadas para cada usuario	Analista TI	Seguridad TI	No	
6.2 f	Limitar acceso y permisos (Funciones)	Analista TI	Seguridad TI	No	
6.2 g	Eliminar acceso al terminar contrato	Analista TI	Seguridad TI	Si	Informe de retiro de accesos
6.2 h	Impedir instalación software no autorizado	Analista TI	Seguridad TI	Si	Matriz de Seguridad TI
6.2 i	Licencia de hardware y software	Analista TI	Seguridad TI	No	
6.2 j	Realizar copia de seguridad	Analista TI	Seguridad TI	Si	Política de Seguridad
6.2 k	Registro actualizado de usuario	Analista TI	Seguridad TI	Si	Listado de usuarios
6.2 l	Cerrar/Bloquear equipos desatendidos	Analista TI	Seguridad TI	Si	Política de Seguridad
6.2 m	Evaluar infraestructura tecnológica (Anual)	Analista TI	Seguridad TI	Si	Política de Seguridad
6.2 n	Identificar y reportar accesos no autorizados	Analista TI	Seguridad TI	Si	Política de Seguridad
6.2 o	Revisar políticas de ciberseguridad	Analista TI	Seguridad TI	Si	Política de Seguridad
6.2 p	Emplear tecnología segura (VPN)	Analista TI	Seguridad TI	Si	Autentificador multifactor
6.2 q	Evitar acceso remoto a la información	Analista TI	Seguridad TI	Si	Política de Seguridad
6.2 r	Realizar inventario tecnológico	Analista TI	Seguridad TI	No	
6.2 s	Restringir conexión de dispositivos personales	Analista TI	Seguridad TI	No	
6.2 t	Evaluar políticas de ciberseguridad	Analista TI	Seguridad TI	Si	Política de Seguridad
6.2 u	Realizar simulacros y ejercicios de tecnología	Analista TI	Seguridad TI	No	
6.2 v	Controles para super usuarios	Analista TI	Seguridad TI	No	

RESULTADOS GLOBALES==========>	60%	

5.5 Vulnerabilidades detectadas

La información contenida en la matriz se obtuvo a partir de un proceso sistemático de revisión documental, entrevistas con el personal responsable y verificación directa de los procedimientos aplicados en las distintas áreas. Este análisis preliminar no solo facilita la preparación para la auditoría de certificación, sino que también contribuye a fortalecer la cultura de seguridad dentro de la empresa. El resultado refleja las brechas que requieren atención:

- Si bien la ubicación del datacenter no es de acceso público, no cuenta con las medidas de seguridad apropiadas para el nivel de criticidad que tiene la infraestructura física.
- No se tienen definidos planes de acción o de contingencia en caso de una perdida de información, daño de los servidores virtualizados.
- La información de la empresa no se encuentra debidamente categorizada, ni existe control de acceso por cargo.
- Dentro de la empresa se fomenta el uso compartido de credenciales sin controles específicos, complicando la trazabilidad de la información.
- No existe un control de las licencias utilizadas para las operaciones normales de la empresa, ni las fechas en las que se deben actualizar o renovar.
- No existe un mecanismo que permita limitar el acceso a los distintos sistemas de acuerdo con el cargo que ocupen.
- La empresa no realiza inventarios periódicos, ni revisión de estados de la infraestructura tecnológica.
- No se mantiene el control para la conexión de dispositivos personales, ni un proceso para autorización y registro de los dispositivos personales.
- Ausencia de plan de simulacros que permita evaluar si es necesaria una capacitación para el personal, ni mucho menos la mejora de las respuestas de los usuarios.

- Dependencia excesiva del personal técnico sin respaldo documental, ni controles a los super usuarios

Las debilidades encontradas están dentro de los vectores de ataque más frecuentes en organizaciones de características similares en la región latinoamericana. (Díaz, 2021)

5.5.1 Evaluación de los riesgos por probabilidad de Ocurrencia

Cada una de las brechas detectadas en el apartado anterior representan un riesgo para el correcto desarrollo de las actividades de la empresa, ya que, al no tener un control establecido, tienen una alta probabilidad de ocurrencia sumado al impacto propio que tendrían a las operaciones comerciales.

Una adecuada gestión de los riesgos permite evaluar y priorizar los riesgos identificados en función de dos variables críticas: la probabilidad de ocurrencia y el impacto potencial sobre la organización, de esta forma se priorizan acciones correctivas y se asignan recursos de manera eficiente. Para cumplir con esto, se genera una Matriz de Probabilidad e Impacto de los Riesgos, misma que facilita la clasificación de riesgos en niveles de criticidad (bajo, medio, alto), lo que permite orientar la toma de decisiones hacia aquellos riesgos que requieren atención inmediata. (Díaz del Castillo Náder & Caballero Olivares, 2020)

Para este método, se asignaron valores de probabilidad e impacto, con esto se calculó el nivel de riesgo mediante su producto y con los umbrales se definió el nivel de riesgo lo que permitió establecer estrategias de respuesta proporcionales al nivel de criticidad, contribuyendo a la resiliencia organizacional y al cumplimiento de los requisitos BASC. (ISO/IEC, 2022; Oswaldo & Reina, 2022)

Para la matriz de probabilidad e impacto de riesgos en Tabla 2, se consideró que de cada una de las no conformidades dentro del SGCS-BASC se obtuvo un riesgo con un impacto y probabilidad de ocurrencia. Las probabilidades fueron asignadas con valores numéricos desde 1 como muy improbable hasta 5 muy probable y de igual

forma el impacto, donde 1 representa impacto bajo hasta 5 que representa un impacto muy crítico.

Tabla 2. Matriz de Probabilidad e Impacto de los Riesgos en la Empresa de Servicios Electrónicos

Matriz de Probabilidad e Impacto de Riesgos			
Riesgo	**Probabilidad**	**Impacto**	**Justificación**
1. Ubicación del datacenter sin medidas de seguridad adecuadas.	4	5	Muy probable que ocurra, el impacto es muy crítico debido a la exposición de la infraestructura física.
2. Ausencia de planes de acción o contingencia en caso de pérdida de información o daño de servidores virtualizados.	4	5	Es probable, ya que muchas empresas no tienen planes adecuados; el impacto es muy crítico si hay pérdida de datos.
3. Falta de categorización de la información y control de acceso por cargo.	4	4	Es probable que ocurra, especialmente si no hay políticas claras; el impacto es crítico debido a la falta de control sobre datos sensibles.
4. Uso compartido de credenciales sin controles específicos.	5	5	Muy probable, ya que a veces se prioriza la comodidad; el impacto es muy crítico debido a la dificultad de rastrear accesos y proteger la información.
5. Sin control del número licencias utilizadas, ni fechas de caducidad	3	4	Moderadamente probable; el impacto es crítico, porque se pierde acceso a las aplicaciones usadas en las operaciones de la empresa.
6. Ausencia de mecanismos para limitar el acceso a sistemas según cargo.	4	4	Muy probable, especialmente en empresas sin políticas de acceso claras; el impacto es crítico, ya que el acceso sin restricciones puede generar fugas de información.
7. Falta de inventarios periódicos y revisión de estados de infraestructura tecnológica.	3	3	Moderadamente probable, pero si no se realiza un inventario, podría haber fallos en la infraestructura no detectados; impacto moderado ya que no afecta directamente en el normal funcionamiento.
8. Control deficiente sobre la conexión de dispositivos personales.	4	3	Muy probable en empresas sin políticas claras; el impacto es moderado debido a riesgos de vulnerabilidad y accesos no autorizados.
9. Ausencia de plan de simulacros y capacitación para el personal.	3	3	Moderadamente probable; el impacto es alto en situaciones de emergencia donde el personal no esté preparado.
10. Dependencia excesiva del personal técnico sin controles ni respaldo documental.	4	4	Muy probable, especialmente en empresas con personal técnico clave sin procedimientos documentados; el impacto es alto por el riesgo de pérdida de conocimiento crítico.

Una vez analizados tanto el impacto como la probabilidad, procedemos a clasificar los riesgos obteniendo producto de estos dos valores y en base a los umbrales establecidos en Tabla 3.

Tabla 3. Umbrales de los Niveles de Riesgo

Tipo de riesgo	Probabilidad vs Impacto
Bajo	1-3
Medio	4-8
Alto	9-14
Muy Alto	15-25

De esta forma podemos categorizar los riesgos en una Matriz de Riesgos que se presenta en la Tabla 4, donde jerarquizamos los riesgos, desde bajo hasta muy alto, y con estos establecer un orden de atención, donde aquellos que se encuentran em Muy alto, son los que requieren atención inmediata, luego proceder con aquellos categorizados como Alto.

Tabla 4. Matriz de Riesgos de la Empresa de Servicios Electrónicos

Probabilidad	**Impacto**				
	Bajo (1)	**Medio (2)**	**Alto (3)**	**Crítico (4)**	**Muy Crítico (5)**
Muy Improbable (1)					
Improbable (2)					
Moderado (3)			Riesgo 7 / Riesgo 9	Riesgo 5	
Probable (4)			Riesgo 8	Riesgo 3 / Riesgo 6 / Riesgo 10	Riesgo 1 / Riesgo 2
Muy Probable (5)					Riesgo 4

Los resultados del diagnóstico evidencian la necesidad impostergable de establecer un sistema integral de gestión de la ciberseguridad. Las brechas detectadas no solo imposibilitan el cumplimiento del marco BASC, sino que también incrementan la exposición a incidentes de alto impacto. Con este análisis técnico se plantearon las

acciones correctivas indicadas en el siguiente apartado, que se centra en la adopción de medidas para el fortalecimiento de la seguridad de la información.

5.6 Implementación de Medidas de Seguridad

Gracias al análisis de la infraestructura tecnológica, se evidenció la necesidad de adoptar medidas orientadas a fortalecer la seguridad de la información dentro de la organización. En este apartado exponen las acciones correctivas alineadas tanto con los requerimientos del SGCS-BASC como con las mejores prácticas establecidas por estándares internacionales en materia de seguridad informática.

La priorización de las acciones se sustenta en dos criterios: el impacto directo sobre la protección de los activos de información y la factibilidad técnica de su aplicación. Este enfoque permite garantizar que las mejoras que se proponen respondan a las exigencias normativas y se integren de manera efectiva en los procesos internos construyendo un sistema robusto y resiliente frente a las amenazas.

Este capítulo se establecen las medidas correctivas necesarias para abordar las brechas identificadas.

5.6.1 Documentación de Matrices Fundamentales

Antes de iniciar el proceso de remediación, es necesario establecer los instrumentos que sirven como base para la elaboración del plan de acción que permiten organizar y priorizar las medidas correctivas asegurando que cada acción esté alineada con los objetivos estratégicos de la organización y a su vez los requisitos del sistema de gestión BASC que proporciona un marco de referencia para definir responsabilidades, plazos y recursos necesarios para su implementación.

5.6.2 Matriz de inventario y criticidad de activos

La elaboración de la matriz de inventario y criticidad de activos permite identificar de manera sistemática todos los activos tecnológicos presentes en la organización, incluyendo equipos físicos, sistemas virtualizados, aplicaciones y servicios críticos para la operación con la finalidad de establecer un registro que refleje la existencia

de cada activo y determine su importancia en relación con la continuidad del negocio de la organización.

La criticidad de los activos se evalúa considerando factores como: su impacto en los procesos operativos, la dependencia de otros sistemas, la sensibilidad de la información que maneja y el grado de exposición a riesgos. Con este análisis, se tiene una visión clara sobre cuáles elementos requieren un mayor nivel de protección y monitoreo, priorizando recursos y esfuerzos en función de su relevancia para la organización. (Echeverría et al., 2024)

Para definir los criterios de forma sistemática, se utilizará el método FMECA (por sus siglas en inglés, Failure Mode, Effects and Criticality Analysis) que permite determinar la criticidad da cada ítem dentro del inventario de activos de la empresa y cuyo cálculo se encuentra especificado en (1) y donde sus variables están definidas en la siguiente matriz en Tabla 5. (D. H. Stamatis, 2003)

$$IC = S \times O \times D \times CI \times TR \tag{1}$$

Tabla 5. Matriz de Criterios del índice de Criticidad de Activos

Matriz de Criterios			
Criterio	**Qué mide**	**1 (Bajo)**	**5 (Alto)**
S – Severidad	Impacto en operaciones si falla	impacto menor	detiene operación o servicios críticos
O – Ocurrencia	Probabilidad de falla	poco probable	falla frecuente / hardware viejo
D – Detección	Facilidad de detectar/prevenir la falla	monitoreo fácil	difícil de predecir
CI – Impacto en Seguridad/Información	Riesgo sobre datos, accesos, grabaciones, evidencia	mínimo	muy alto
TR – Tiempo de recuperación	Qué tan rápido se recupera	minutos	días

Finalmente, del valor obtenido en la ecuación del índice de criticidad (1) y que se encuentran representados en Tabla 6, se definirán con base en los criterios establecidos por los siguientes rangos

- Crítico: IC>300
- Alto: 120<IC≤300
- Medio: 50<IC≤120
- Bajo: IC≤50

Tabla 6. Matriz de Índices de Criterios de Criticidad del Inventario TI de la Empresa de Servicios Electrónicos

Matriz de Índices de Criticidad						
Activo	**S**	**O**	**D**	**CI**	**TR**	**IC**
Hipervisor	5	3	3	5	4	**900**
Hipervisor	5	3	3	5	4	**900**
Server Físico	4	3	3	4	4	**576**
NAS Synology	4	3	2	4	3	**288**
Central Telefónica	3	2	3	2	3	**108**
Teléfonos IP	2	2	3	1	2	**24**
NVR	4	3	2	4	4	**384**
Cámaras IP	3	3	2	4	3	**216**
Reloj Biométrico	2	2	2	1	2	**16**
Microsoft 365	5	2	5	5	5	**1250**
Monitoreo impresión	2	2	3	1	2	**24**
vCenter	5	3	3	5	4	**900**
Antivirus	4	3	3	5	3	**540**
Gestor de Impresión	2	2	3	1	2	**24**
ERP	5	2	3	5	5	**750**
Respaldos	5	3	3	5	5	**1125**
Directorio Activo	5	3	3	5	4	**900**
Directorio Activo 2	4	2	3	4	3	**288**
Mesa de Ayuda Interna	2	2	2	1	2	**16**
Mesa de Ayuda Clientes	3	2	3	3	2	**108**
Base de Datos movimientos	3	2	3	2	3	**108**
Switch Core	5	3	3	5	5	**1125**
Switch Servidores	5	3	3	5	5	**1125**
Switch Técnico	3	2	3	2	2	**72**
Switch Administrativo	2	2	3	1	2	**24**
Switch Comercial	2	2	3	1	2	**24**
Firewall Fortinet	5	3	3	5	5	**1125**
Router Frontera	5	3	3	5	5	**1125**
AP Corporativo	3	2	3	2	2	**72**
AP Comercial	2	2	3	1	2	**24**
AP Técnico	2	2	3	1	2	**24**
Monitoreo Activos	2	2	2	1	2	**16**
Sistema de Activos	2	2	2	1	2	**16**

Con estos índices, clasificamos la criticidad de los ítems dentro del inventario de activos de la Empresa de Servicios Electrónicos y que se encuentran representados en la matriz de la Tabla 7.

Tabla 7. Matriz de Criticidad del Inventario de Activos de la Empresa de Servicios Electrónicos

Matriz Nivel de Criticidad de Activos					
Categoría	**Activo / Sistema**	**Descripción**	**Ubicación**	**Responsable**	**Criticidad**
Servidor	Hipervisor	Servidor Virtualizado 1	Rack TI	Analista TI	Crítico
Servidor	Hipervisor	Servidor Virtualizado 2	Rack TI	Analista TI	Crítico
Servidor	Server Local	Almacenamiento para Vcenter	Rack TI	Analista TI	Crítico
Servidor	NAS Synology	Almacenamiento	Rack TI	Analista TI	Alto
VoIP	Central Telefónica	Central de telefonía IP	Rack TI	Analista TI	Medio
VoIP	Teléfonos IP	Teléfono IP x 15	Puesto Asignado	Analista TI	Bajo
Seguridad	NVR	Central de cámaras de seguridad	Rack TI	Analista TI	Crítico
Seguridad	Cámaras IP	Cámara IP de seguridad x 16	Puesto Asignado	Analista TI	Alto
Seguridad	Reloj Biométrico	Control de asistencia	Puesto Control	Proveedor	Bajo
Aplicación	Microsoft 365	Correo y aplicaciones corporativas	Nube	Analista TI	Crítico
Aplicación	Monitoreo equipos de impresión	Monitoreo de Impresoras de clientes, arrendadas y propias	Nube	Analista TI	Bajo
Software	vCenter	Gestión De Servidores Virtuales	Servidor Virtual	Analista TI	Crítico
Software	Antivirus	Antivirus	Servidor Virtual	Analista TI	Crítico
Software	Gestión de impresión	Software de gestión de impresión y control de accesos	Servidor Virtual	Analista TI	Bajo
Software	ERP	ERP	Servidor Virtual	Desarrollador	Crítico
Software	Backups	Respaldos de servidores y bases de datos	Servidor Virtual	Analista TI	Crítico
Software	Directorio Activo	Registro de usuarios y equipos	Servidor Virtual	Analista TI	Crítico
Software	Directorio Activo 2	Respaldo de registro de usuarios y equipos	Servidor Virtual	Analista TI	Alto
Software	Mesa de Ayuda Interna	Mesa de Ayuda Tecnología	Servidor Virtual	Analista TI	Bajo
Software	Mesa de Ayuda Clientes	Mesa de Ayuda Clientes	Servidor Virtual	Analista TI	Medio

Software	Base de Datos movimientos	Base de datos de activos e historial de movimientos	Servidor Virtual	Desarrollador	Medio
Software	Sistema de Activos	Movimientos de Inventario	Servidor Virtual	Desarrollador	Crítico
Software	Monitoreo de Activos	Monitoreo de Activos Registrados	Servidor Virtual	Analista TI	Crítico
Red	Switch L3	Switch Core	Rack TI	Analista TI	Medio
Red	Switch L3	Switch Servidores	Rack TI	Analista TI	Bajo
Red	Switch L3	Switch Departamento Tecnico	Rack TI	Analista TI	Bajo
Red	Switch L3	Switch Administrativo	Oficina Corporativas	Analista TI	Crítico
Red	Switch L3	Switch Comercial	Oficina Comercial	Analista TI	Crítico
Red	Firewall Fortinet	Seguridad perimetral	Rack TI	Proveedor	Medio
Red	Router	Router de Frontera	Rack TI	Proveedor	Bajo
Red	Access Point	WiFi corporativa	Oficina Corporativas	Analista TI	Bajo
Red	Access Point	WiFi Comercial	Oficina Comercial	Analista TI	Bajo
Red	Access Point	WiFi Departamento Técnico	Departamento Técnico	Analista TI	Bajo

En un entorno corporativo cada vez más expuesto a amenazas digitales, la gestión proactiva de activos críticos se convierte en un factor determinante para la sostenibilidad y competitividad de la organización. Teniendo esto en cuenta, se debe considerar una frecuencia para respaldar la información, que esté relacionada con la criticidad de los activos, considerando la importancia que cada activo tiene dentro de la operación normal de la empresa, por lo que se plantea el uso de una matriz de frecuencia de respaldos, tomando la estructura de la Matriz de Criticidad de Activos en Tabla 7 y considerando las siguientes frecuencias.

- Nivel Crítico: Diario / en tiempo real (si aplica)
- Nivel Alto: Semanal
- Nivel Medio: Semanal o Quincenal según tipo de información
- Nivel Bajo: Mensual o bajo demanda

Tomando en consideración los criterios establecidos, se genera la matriz de frecuencias de respaldos en la Tabla 8.

Tabla 8. Matriz de Frecuencia Respaldos Considerando la Criticidad del Activo en la Empresa de Servicios Electrónicos

c				
Categoría	**Activo / Sistema**	**Responsable**	**Criticidad**	**Frecuencia**
Servidor	Hipervisor	Analista TI	Crítico	Diario
Servidor	Hipervisor	Analista TI	Crítico	Diario
Servidor	Server Local	Analista TI	Crítico	Diario
Servidor	NAS Synology	Analista TI	Alto	Semanal
VoIP	Central Telefónica	Analista TI	Medio	Semanal
Seguridad	NVR	Analista TI	Crítico	Diario
Seguridad	Reloj Biométrico	Proveedor	Bajo	Mensual
Aplicación	Microsoft 365	Analista TI	Crítico	Diario
Aplicación	Monitoreo equipos de impresión	Analista TI	Bajo	Mensual
Software	vCenter	Analista TI	Crítico	Diario
Software	Antivirus	Analista TI	Crítico	Diario
Software	Gestión de impresión	Analista TI	Bajo	Mensual
Software	ERP	Desarrollador	Crítico	Diario
Software	Backups	Analista TI	Crítico	Diario
Software	Directorio Activo	Analista TI	Crítico	Diario
Software	Directorio Activo 2	Analista TI	Alto	Semanal
Software	Mesa de Ayuda Interna	Analista TI	Bajo	Mensual
Software	Mesa de Ayuda Clientes	Analista TI	Medio	Semanal
Software	Base de Datos Movimientos	Desarrollador	Crítico	Diario
Software	Sistema de Activos	Desarrollador	Crítico	Diario
Software	Monitoreo de Activos	Analista TI	Crítico	Diario
Red	Switch Core	Analista TI	Critico	Diario
Red	Switch Servidores	Analista TI	Alto	Semanal
Red	Switch Dep. Técnico	Analista TI	Bajo	Mensual
Red	Switch Área Administrativa	Analista TI	Bajo	Mensual
Red	Switch Área Comercial	Analista TI	Bajo	Mensual
Red	Firewall Fortinet	Proveedor	Medio	Semanal
Red	Router Frontera	Proveedor	Alto	Semanal
Red	Access Point Área Administrativa	Analista TI	Bajo	Mensual
Red	Access Point Área Comercial	Analista TI	Bajo	Mensual
Red	Access Point Dep. Técnico	Analista TI	Bajo	Mensual

Una vez definida la criticidad de los activos, es necesario abordar los cargos de la organización y determinar accesos de acuerdo con los niveles de criticidad.

5.6.3 Matriz de Criticidad de Cargos

La matriz de criticidad de cargos se diseñó conforme a los lineamientos establecidos en la norma ISO/IEC 27001:2022, que define los requisitos para la gestión de la seguridad de la información, y siguiendo la guía metodológica para la evaluación de

riesgos descrita en ISO/IEC 27005:2022, la cual proporciona un enfoque sistemático para identificar, analizar y tratar riesgos relacionados con la información. Este instrumento tiene como propósito determinar el nivel de exposición al riesgo asociado a cada cargo dentro de la organización, permitiendo implementar medidas de control proporcionales y coherentes con el enfoque de gestión basado en riesgos que exige el estándar internacional. (ISO/IEC, 2022)

La metodología aplicada contempla la valoración de los cargos en función de criterios previamente definidos que reflejan el grado de exposición frente a amenazas que puedan comprometer la confidencialidad, integridad y disponibilidad de la información. Cada criterio se califica en una escala de 0 a 3, donde el valor cero indica que el criterio no aplica o que la exposición al riesgo es nula y 3 es alto. La suma de los valores asignados permite clasificar cada cargo en niveles de criticidad baja, media o alta, lo que orienta la definición de controles específicos relacionados con accesos, privilegios, responsabilidades, capacitación y auditorías internas. Este enfoque asegura que las decisiones sobre seguridad se fundamenten en un análisis objetivo y alineado con las mejores prácticas internacionales. (ISO/IEC, 2022; Romero, n.d.)

Se define la escala de la siguiente forma, tal como se indica en la Tabla 9 y donde los criterios de evaluación se establecen a continuación.

Criterios de

- Acceso a información sensible
- Acceso a sistemas críticos (ERP, servidores, NVR, WMS, etc.)
- Privilegios técnicos o administrativos
- Impacto operacional en caso de error
- Acceso físico a áreas críticas (datacenter, almacén, servidores)
- Rol en la cadena logística o procesos claves

Tabla 9. Descripción específica de los valores de la escala de criticidad según la ISO 27005

Escala de valores	
Valor	**Descripción**

0	No aplica. Sin acceso, exposición o impacto.
1	Bajo. Acceso mínimo o impacto limitado.
2	Medio. Acceso moderado, posible impacto relevante.
3	Alto. Exposición directa, acceso privilegiado o impacto crítico.

Una vez establecidos los criterios y la escala, se plantea los niveles de criticidad, en la Tabla 10, con base en los rangos según la sumatoria de los valores en cada criterio.

Tabla 10. Rangos para Establecer el Nivel de Criticidad con Base en la Sumatoria de los Valores de los Criterios

Rangos Para los Niveles de Criticidad de Cargos		
Total	**Criticidad**	**Significado**
0 – 4	Baja	Exposición mínima, controles básicos.
5 – 10	Media	Riesgo moderado, controles específicos.
11 – 18	Alta	Alta exposición, requiere monitoreo exhaustivo y controles avanzados

Con estos criterios, se procede a evaluar a cada uno de los cargos establecidos en la Empresa de Servicios Electrónicos, considerando los valores y umbrales planteados anteriormente en la Tabla 10 y con esto se construye la matriz de Evaluación de Criterios por Cargo

Tabla 11. Totales de los Niveles de Criticidad Según cada Cargo

Matriz de Evaluación de Criterios por Cargo							
Cargo	**Info. sensible**	**Sistemas críticos**	**Privilegios técnicos**	**Impacto operación**	**Acceso físico áreas críticas**	**Cadena logística**	**Total**
Gerencia	3	3	1	3	1	3	14
Presidencia	3	3	0	3	1	2	12
Servicios	3	3	2	2	3	1	14
Analista TI	3	3	3	3	3	2	17
Desarrollador TI	3	3	2	3	1	3	15
Contabilidad	3	2	0	3	0	2	10
Recursos Humanos	2	2	0	2	0	1	7
Logística	2	2	0	3	1	3	11
Jefes de Área	2	2	0	2	0	1	7
Departamento técnico	0	0	0	1	2	0	3
Arriendos	2	2	0	2	0	1	7
Recepción	0	0	0	1	2	1	4
Despachos	0	0	0	1	0	3	4
Auxiliar de Limpieza	0	0	0	0	2	0	2

Finalmente, se establece la Matriz de Criticidad de Cargos en la Tabla Tabla 12, con referencia en la Criticidad comparando el valor en la columna Total obtenido en Tabla Tabla 10 y el Total en la Tabla 11, con este se encuentra a cuál de los 3 rangos de criticidad pertenece, y, este rango, categoriza a cada cargo.

Tabla 12. Matriz de Criticidad de los Cargos en la Empresa de Servicios Electrónicos

Matriz de Accesos por Criticidad de Cargos						
Cargo	**Criticidad**	**Tipo de Info. Permitida**	**Nivel**	**Sistemas Autorizados**	**Restriccion**	**Justificación**
Gerencia	**Alta**	Información estratégica financiera	Lectura / Aprobación	ERP, CRM, Documentación de estrategia	Sin acceso técnico	Información para decisiones, administración técnica limitada
Presidencia	**Alta**	Información financiera legal	Lectura / Aprobación	Información Legal y Financiera, ERP	Sin acceso técnico	Información para control administrativo
Coordinación	**Alta**	Información estratégica y técnica	Lectura / Escritura	Documentación Estratégica, documentación técnica	Sin acceso técnico	Gestiona las decisiones desde Gerencia hacia TI y Arriendos
Analista TI	**Alta**	Infraestructura servidores redes	Administrador	Servidores, AD, Backups, Seguridad	Auditoría obligatoria	Administra la infraestructura crítica
Desarrollador	**Alta**	ERP, Activos	Super usuario	Aplicación ERP, Bases de Datos	Auditoría obligatoria	Administra la infraestructura crítica
Contabilidad	Media	Información contable, tributaria	Lectura / Escritura	ERP Financiero	Sin acceso técnico	Maneja datos financieros críticos
Recursos Humanos	Media	Datos personales, nómina	Lectura / Escritura	Sistema RRHH	Sin acceso financiero ni técnico	Maneja información sensible del personal
Logística	Alta	Información de Cadena de suministros	Lectura / Escritura	Movimientos de inventario, ERP módulos operativos	Sin acceso financiero ni técnico	Maneja el abastecimiento y distribución del inventario
Jefes de Área	Media	Información operativa	Lectura / Escritura en su área	CRM, ERP Módulos de Facturación, Activos	Sin acceso a datos críticos	Requiere supervisión operativa
Dep. técnico	Baja	Datos básicos para funciones	Lectura	Sistema operativo correspondiente	Sin acceso confidencial	Acceso mínimo necesario
Operativa	Media	Documentos internos	Lectura / Escritura limitada	ERP Módulos de Facturación, Activos, Mesa de Ayuda Clientes	Sin acceso financiero	Acceso básico para tareas administrativas

Recepción	Baja	Información operativa	Lectura / Escritura	Activos, Mesa de Ayuda Interna	Sin acceso financiero ni técnico	Acceso básico para tareas administrativas
Despachos	Baja	Información operativa	Lectura	Solo red empresarial	Sin acceso confidencial	Acceso mínimo necesario
Auxiliar de Limpieza	Baja	Politicas generales	Lectura	Solo red empresarial	Sin acceso confidencial	Acceso mínimo necesario
Visitantes / Proveedores	Sin accesos	Ninguna	Ninguna	Solo red invitados	Sin acceso corporativo	Prevención de riesgos externos

5.6.4 Matriz de Inventario y Clasificación de Información

La Matriz de Inventario y Clasificación de la Información constituye un instrumento fundamental para la gestión segura de los activos informativos de la organización, en cumplimiento de los lineamientos de la Norma BASC V6 y la Ley Orgánica de Protección de Datos Personales (LOPDP) vigente en Ecuador. Su propósito es identificar, categorizar y controlar la información que se genera, procesa y almacena, garantizando la confidencialidad, integridad y disponibilidad, así como la protección de datos personales y sensibles conforme a la normativa aplicable. La matriz cumple una función estratégica en la gestión del riesgo, ya que permite priorizar la protección de activos críticos y aplicar controles proporcionales al nivel de sensibilidad de la información; ayuda en el cumplimiento normativo al facilitar la demostración de conformidad con BASC y la LOPDP, asegurando que la organización aplica principios de minimización, seguridad y control de acceso y, además brinda soporte a políticas y procedimientos porque actúa como evidencia documental para la política de clasificación y el procedimiento de gestión de accesos, sirviendo de base para auditorías internas y externas. (ISO/IEC, 2022a; LOPDP, 2021; WBO, 2022)

Para esta matriz de inventario se consideran los siguientes campos:

- Activo de información (nombre del archivo, base de datos, sistema).
- Tipo de información (personal, financiera, operativa, pública).

- Formato (digital, físico).
- Ubicación (servidor, nube, archivo físico).
- Responsable (persona o área).
- Nivel de criticidad (Crítico, Confidencial, Público).
- Controles aplicados (cifrado, MFA, acceso restringido).

Con esta base, se procede a definir los niveles de criticidad de la información categorizándola en tres niveles y posteriormente se crea la matriz de inventario en la Tabla 13:

- Crítico: datos personales, credenciales, información financiera y datos relacionados con la certificación BASC.
- Confidencial: información operativa interna y procesos logísticos.
- Público: información divulgable sin riesgo.

Tabla 13 Matriz de Inventario y Clasificación de la Información de la Empresa de Servicios Electrónicos

Matriz de Inventario y Clasificación de la Información						
Activo de Información	**Tipo**	**Formato**	**Ubicación**	**Responsable**	**Criticidad**	**Controles Aplicados**
Reportes internos en Power BI	Operativa	Digital	Power BI Cloud	Analista TI	Confidencial	MFA, acceso por rol
Reportes clientes en Power BI	Operativa	Digital	Power BI Cloud	Analista TI	Confidencial	MFA, acceso por rol
Bases de datos	Personal/Financ.	Digital	Servidor local	Desarrollador TI	Crítico	Cifrado, MFA, backup
Políticas, procesos, plantillas y matrices	Documentación	Digital	SharePoint	Analsita Procesos	Confidencial	Control de permisos
Respaldos empleados cesantes	Personal	Digital	NAS	Analista TI	Crítico	Cifrado, acceso restringido
Correos electrónicos	Personal/Operat.	Digital	Office 365	Analista TI	Confidencial	MFA, monitoreo
Facturación y compras (ERP)	Financiera	Digital	Servidor local	Desarrollador TI	Crítico	Cifrado, acceso por rol
Contratos de arrendamiento clientes	Legal	Físico y Dig.	Archivo físico / Teams	Analista Procesos	Confidencial	Control físico, permisos
Manuales operativos	Operativa	Físico	Archivo central	Encargado Procesos	Confidencial	Control físico
Contratos empleados y estatutos	Legal	Físico	Archivo físico	Analista Procesos	Confidencial	Control físico

Página web corporativa	Pública	Digital	Hosting externo	Analista TI	Público	Monitoreo
Políticas Comerciales	Publica	Digital	Hosting externo	Presidencia	Público	Monitoreo
Guías de remisión	Logística/Operativa	Fisico	Archivo físico	Jefe de Logistica	Confidencial	Control físico
Actas de asignación y retiro de equipos	Documentación Activos	Digital	NAS	Desarrollador TI	Confidencial	Acceso por rol
Análisis y reportes financieros	Financiera	Digital	OneDrive	Contador	Crítico	Cifrado, MFA, backup
Estrategias comerciales	Comercial	Digital	OneDrive	Marketing	Confidencial	Acceso por rol, SharePoint
Archivo maestro de credenciales	Acceso privilegiado	Digital	OneDrive	Analista TI	Crítico	Cifrado, acceso restringido, MFA

5.7 Controles Implementados para el Cumplimiento con el SGCS-BASC Para Seguridad de la Información

La implementación efectiva de un Sistema de Gestión en Control y Seguridad (SGCS) conforme a la Norma y Estándares BASC requiere del establecimiento de un conjunto estructurado de controles diseñados para proteger los procesos críticos, los activos de información y la integridad de la cadena logística. Estos controles constituyen la base operativa del sistema y permiten garantizar que las actividades, recursos y tecnologías involucradas en las operaciones de la organización se desarrollen bajo criterios de seguridad verificables, medibles y auditables.

El establecimiento de controles implica definir, documentar, implementar y mantener medidas específicas que reduzcan los riesgos identificados durante el proceso de análisis. De acuerdo con BASC, los controles deben estar alineados con los objetivos del SGCS, estar fundamentados en políticas institucionales y responder a amenazas que puedan afectar a la continuidad de negocio.

5.7.1 Proteger la información crítica y los activos tecnológicos - 6.1 c

Desde el punto de vista del espacio disponible y su distribución, se recomienda la construcción de un espacio cerrado con la seguridad correspondiente de forma que se pueda mantener el control de acceso al datacenter se debe encontrar completamente aislado del personal, y que, únicamente el personal autorizado pueda tener acceso.

A corto plazo, se inicia por categorizar la infraestructura tecnológica como crítica, esto documentado en la Matriz Nivel de Criticidad de Activos en Tabla 4 y se debe establecer, dentro de la política en Anexo: TI-SEG-POL-04, que el acceso al rack del datacenter es restringido y su manipulación está completamente prohibida determinando que, únicamente Analista TI y en su ausencia el Desarrollador TI tienen permitida su gestión, y además, se tiene que controlar el rack mediante una cámara de seguridad que permita identificar si se realiza alguna acción no autorizada. Este proceso de remediación se alinea con el control de accesos estipulado en el estándar BASC y constituye una práctica recomendada por la norma ISO/IEC 27002 [1], [2].

5.7.2 Criterios de seguridad (Proteger y recuperar) – 6.2 a

Este plan tiene como propósito definir las directrices, actividades y responsabilidades necesarias para implementar dicho control de manera estructurada y medible. Su ejecución asegura que la organización cuente con criterios formales de seguridad, mecanismos de protección y procedimientos de respaldo y recuperación que permitan minimizar las interrupciones operativas causadas por fallas tecnológicas, incidentes de seguridad o eventos no planificados.

La implementación de este control se fundamenta en tres pilares principales:

- Identificación y clasificación de los sistemas de TI, para determinar su criticidad y con esto priorizar acciones de protección, esto se lo logra gracias a la Matriz de Criticidad realizada en Tabla 7.

- Establecimiento de criterios de seguridad documentados, que orienten la protección técnica, operativa y administrativa de los sistemas, establecido en el Anexo Anexo: TI-SEG-CRS-01.
- Definición de mecanismos de recuperación, que garanticen la continuidad del negocio mediante estrategias de respaldo y restauración verificadas establecidas en el Anexo: TI-BCP-PR-01 Proceso de respaldo y restauración.

Este enfoque permite fortalecer la infraestructura tecnológica, reducir riesgos asociados a la pérdida o alteración de información y dar cumplimiento a los requisitos formales de auditoría BASC, al asegurar que los controles se encuentren implementados, mantenidos y respaldados con evidencia documentada todo esto planteado en el Anexo: TI-BCP-PR-02.

5.7.3 Clasificar información según criticidad – 6.2 c

En cumplimiento de la Norma BASC V6 y la Ley Orgánica de Protección de Datos Personales vigente en Ecuador, la organización ha iniciado la implementación del control orientado a la clasificación de la información y la definición de políticas de acceso basadas en niveles de criticidad. Este proceso, documentado en Anexo: TI-INF-POL-02, busca garantizar la confidencialidad, integridad y disponibilidad de los datos, así como el respeto a los derechos de los titulares de información personal. La implementación comprende las siguientes acciones estratégicas:

5.7.3.1 Inventario y análisis de información

Se ha realizado la identificación de todos los activos de información, incluyendo datos personales, operativos y estratégicos, con el fin de evaluar su nivel de criticidad conforme a los criterios establecidos por BASC y la LOPDP.

5.7.3.2 Clasificación por niveles de criticidad

La información se clasifica en una Matriz de Inventario y Clasificación de la Información, según lo establecido para la Tabla 10

5.7.3.3 Definición de políticas de acceso

Se han establecido políticas que regulan el acceso a la información según su clasificación, aplicando el principio de mínimo privilegio y la necesidad operativa. Para los niveles críticos, se han implementado mecanismos de autenticación robusta (incluyendo MFA), cifrado y registro en bitácoras para garantizar trazabilidad.

5.7.3.4 Cumplimiento normativo y controles técnicos

Las medidas adoptadas aseguran el cumplimiento de los principios de la LOPDP, tales como minimización de datos, consentimiento informado y seguridad reforzada para datos sensibles. Asimismo, se han incorporado controles exigidos por BASC V, como monitoreo continuo y auditorías periódicas.

5.7.3.5 Capacitación y concienciación

El personal involucrado ha recibido formación sobre la correcta aplicación de la clasificación, el manejo seguro de la información y las responsabilidades derivadas del acceso autorizado.

5.7.3.6 Monitoreo y mejora continua

Se ha establecido un sistema de seguimiento que permite evaluar la efectividad de las políticas y procedimientos, garantizando su actualización conforme a cambios normativos o riesgos emergentes.

Con estas acciones, la organización asegura que la gestión de la información se realice bajo estándares internacionales y en estricto apego a la legislación ecuatoriana, fortaleciendo la seguridad y la confianza en sus procesos.

5.7.4 Cuentas asignadas para cada usuario - 6.2 e

Con el fin de cumplir con el control relacionado con el uso de cuentas individuales y mecanismos de autenticación seguros, la organización debe garantizar que cada usuario cuente con credenciales propias, intransferibles y controladas, así como

mecanismos de actualización y revocación que aseguren la protección de la información y la trazabilidad de las acciones realizadas en los sistemas corporativos.

Actualmente se han identificado prácticas que requieren fortalecimiento, tales como el uso constante de cuentas compartidas, credenciales con vigencia indefinida, o falta de evidencia documental sobre la rotación de contraseñas. Para eliminar estos riesgos y asegurar el cumplimiento del estándar BASC, dentro de la política de Seguridad TI en el Anexo: TI-SEG-POL-04, se establece que las credenciales de acceso a los sistemas que emplea la empresa son individuales y la transferencia de estas se considera una falta grave, las características para el uso de contraseñas seguras y la autenticación multifactor en sistemas críticos.

5.7.5 Limitar acceso y permisos (Funciones) – 6.2 f

En el contexto del sistema BASC, la gestión de accesos basada en roles es una práctica esencial para garantizar la seguridad de la información y la integridad de los procesos. Limitar los permisos de los usuarios según sus funciones y revisarlos periódicamente responde al principio de mínimos privilegios, reconocido por estándares como ISO/IEC 27001:2022 y ISO/IEC 27005:2022, que establecen la necesidad de aplicar controles proporcionales al nivel de riesgo.

La Matriz de Criticidad de Cargos en Tabla 12 se convierte en una herramienta estratégica para este propósito, ya que permite clasificar los roles según su exposición y definir políticas de acceso coherentes con el nivel de criticidad identificado. Siguiendo estos parámetros y haciendo uso del Directorio Activo se aplican los permisos y accesos basados en los niveles de criticidad. Para documentar el cumplimiento, se realizan auditorías a los permisos y accesos otorgados a los miembros de la empresa, para esto se presenta un modelo de Registro de Revisión Periódica de Accesos Empresa de Servicio Electrónicos en Anexo: TI-INF-REG-02, de forma que se documente en concordancia con lo establecido en la Política de Gestión de Accesos y Privilegios en Anexo: TI-GAP-POL-01.

5.7.6 Licencia de hardware y software – 6.2 i

El uso de hardware y software licenciados y actualizados es un requisito fundamental para garantizar la seguridad de la infraestructura tecnológica y reducir la exposición a amenazas informáticas. Este control, establecido por el estándar BASC, busca asegurar que la organización mantenga un entorno confiable, cumpliendo con las disposiciones legales y las mejores prácticas internacionales en materia de ciberseguridad. Sin embargo, la ausencia de registros documentales que evidencien la vigencia de las licencias y el estado de actualización representa una brecha significativa que debe ser corregida para cumplir con los requisitos de auditoría y fortalecer la trazabilidad del sistema de gestión.

5.7.6.1 Inventario Documentado de Hardware y Software Licenciado

Elaborar un registro formal que incluya todas las aplicaciones y sistemas utilizados en la organización, utilizando una Matriz De Control De Licencias en Tabla 14, donde se lleva mantiene registrados los tipos de licencia y sus fechas de vencimiento.

Tabla 14. Matriz de Control de Licencias de la Empresa de Servicios Electrónicos

Activo / Sistema	Responsable	Criticidad	Tipo	Fecha de Vencimiento	Renovación
Microsoft 365	Analista TI	Crítico	Subscripción	09-10-25	Anual
Monitoreo equipos de impresión	Analista TI	Bajo	Subscripción	11-10-25	Mensual
vCcenter	Analista TI	Crítico	Perpetua	-	-
Antivirus	Analista TI	Crítico	Licencia		Anual
Gestión de impresión	Analista TI	Bajo	NFT	10-07-25	Semestral
ERP	Desarrollador	Crítico	Licencia	10-03-26	Anual
Backups	Analista TI	Crítico	Licencia	23-02-25	Mensual
Directorio Activo	Analista TI	Crítico	OEM	-	-
Directorio Activo 2	Analista TI	Alto	OEM	-	-
Mesa de Ayuda Interna	Analista TI	Bajo	Software Libre	-	-
Mesa de Ayuda Clientes	Analista TI	Medio	Licencia	14-11-25	Anual
Base de Datos	Desarrollador	Medio	DesarrolloPropio	-	-
Sistema de Activos	Desarrollador	Crítico	DesarrolloPropio	-	-
Monitoreo de Activos	Analista TI	Crítico	Software Libre	-	-

Este inventario debe mantenerse actualizado y vinculado a la Matriz de Criticidad de Activos, para priorizar aquellos sistemas que soportan procesos críticos.

5.7.6.2 Política de Licenciamiento y Actualización

Se redacta una política que establezca la obligatoriedad de utilizar software original, mantener licencias vigentes y aplicar actualizaciones de seguridad en plazos definidos. Esta política debe incluir responsabilidades del área de TI y mecanismos de control y se documenta en Anexo: TI-LAC-POL-01.

5.7.6.3 Procedimiento de Verificación Periódica

Implementar revisiones trimestrales para confirmar la vigencia de las licencias y el estado de actualización de los sistemas. Cada revisión debe documentarse en un Registro de Verificación de Licencias y Actualizaciones en Anexo TI-LAC-REG-01, que servirá como evidencia para auditorías BASC.

5.7.7 Realizar inventario tecnológico – 6.2 R

Con el propósito de garantizar la integridad, trazabilidad y seguridad de la infraestructura tecnológica de la organización, se establece la obligación de controlar mediante la realización de inventarios periódicos todos los medios, dispositivos y equipos que conforman la infraestructura informática.

Los inventarios deberán efectuarse con una frecuencia definida por la empresa en el Anexo: TI-GAT-POL-01, asegurando la actualización constante de la información documentada sobre la ubicación, estado y uso de cada equipo. Este control contribuye a la gestión del riesgo, la prevención de incidentes de seguridad y el cumplimiento de los requisitos legales y normativos aplicables, tal como lo establece la Norma Internacional BASC en sus apartados relacionados con infraestructura operacional, seguridad de la información y gestión de activos tecnológicos y debe documentarse el proceso en el registro como se presenta en Anexo: TI-GAT-RG-01.

En cuanto a la eliminación, desecho o disposición final de los equipos informáticos que hayan cumplido su ciclo de vida útil, la organización deberá aplicar procedimientos seguros, documentado en el Anexo: TI-GAT-PR-01, que garanticen la protección de la información contenida en dichos dispositivos, evitando cualquier acceso no autorizado.

5.7.8 Restringir conexión de dispositivos personales – 6.2 s

En la documentación empresarial no existía un mecanismo formal y documentado que controle o limite la conexión de dispositivos personales (BYOD) o periféricos no autorizados a equipos que forman parte de la infraestructura tecnológica de la empresa. Esto representa un riesgo de seguridad relacionado con la introducción de malware, fuga de información o compromisos no autorizados dentro de la red corporativa.

Establecer controles técnicos y administrativos que impidan la conexión y uso de dispositivos personales o periféricos no autorizados en equipos de la organización, garantizando la protección de la infraestructura informática y la información. Crear y aprobar la Política De Control De Dispositivos Externos Y Periféricos No Autorizados en Anexo: TI-BCP-POL-01 que prohíba el uso de dispositivos USB personales, discos externos, teléfonos, adaptadores y periféricos no autorizados.

5.7.9 Realizar simulacros y ejercicios de tecnología – 6.2 u

La organización establece y ejecuta ejercicios prácticos y simulacros periódicos orientados a evaluar la eficacia de las medidas de seguridad implementadas en las tecnologías de la información según lo establecido en la política documentada en el Anexo: TI-SIM-POL-01. Estos ejercicios deberán permitir identificar oportunidades de mejora, validar la capacidad de respuesta ante incidentes, garantizar la adecuada coordinación entre los equipos involucrados y verificar que los procedimientos establecidos cumplen con los objetivos de continuidad y protección de la información.

Todas las actividades deberán ser planificadas, documentadas y evaluadas, dejando evidencia de los resultados obtenidos, acciones correctivas y lecciones aprendidas, con el propósito de fortalecer el nivel de madurez del sistema de gestión de seguridad y asegurar que los controles operan de manera efectiva.

5.7.10 Controles para super usuarios – 6.2 v

Para garantizar la integridad y disponibilidad de los sistemas críticos, se implementarán controles específicos sobre cuentas con privilegios elevados (superusuarios), alineados con los principios de seguridad establecidos en BASC. Se establecerán mecanismos de gestión centralizada para las credenciales asociadas a cuentas privilegiadas, asegurando su continuidad únicamente en equipos activos y bajo condiciones previamente definidas por la política corporativa de seguridad. Dichos mecanismos incluirán la aplicación de controles de ciclo de vida, tales como validación periódica de vigencia, rotación segura de contraseñas y monitoreo de uso, con el objetivo de prevenir accesos no autorizados y reducir riesgos derivados de credenciales obsoletas o inactivas, esto se encuentra documentado en la política en Anexo: TI-GSU-POL-01 y se detalla también en el Anexo: TI-GSU-PR-01 el proceso para la adecuada gestión.

Adicionalmente, el Anexo se incorpora la implementación del procedimiento de contingencia que permitan la preservación temporal de credenciales en escenarios donde la continuidad sea indispensable para la operación, garantizando que esta práctica se realice bajo autorización formal, registro en sistemas de auditoría y cumplimiento estricto de los lineamientos BASC sobre control de accesos privilegiados.

5.8 Plan de Implementación de Controles

Tiene como objetivo el reducir la exposición a riesgos críticos, identificados en la matriz de riesgos, mediante la implementación de controles técnicos, administrativos y físicos, priorizando aquellos con mayor nivel de criticidad. Esto

permitiría enfocarse primero en aquellos riegos clasificados con un riego Muy Alto, siguiendo lo establecido en el plan de implementación en el Anexo: TI-PIC-PR-01.

Tabla 15. Cronograma de Implementación de los Controles Establecidos para el Cumplimiento del Estándar BASC en el Apartado de Seguridad de la Información

Riesgo Crítico	Control BASC	Acción Específica	Prioridad	Plazo
Uso compartido de credenciales	6.2 e, 6.2 f, 6.2 v	Implementar autenticación individual, MFA, prohibir credenciales compartidas	Alta	30 días
Ausencia de planes de contingencia	6.2 a, 6.2 u	Diseñar plan de recuperación ante desastres, realizar simulacros	Alta	45 días
Ubicación del datacenter sin seguridad	6.1 c	Instalar sistemas de control físico (acceso restringido, CCTV, alarmas)	Alta	60 días
Falta de categorización de información	6.2 a	Clasificar información según criticidad, definir políticas de acceso	Alta	60 días
Ausencia de mecanismos para limitar acceso	6.2 f	Implementar RBAC (Role-Based Access Control)	Alta	60 días
Dependencia excesiva del personal técnico	6.2 v	Documentar procedimientos críticos, crear cuentas individuales	Media	90 días
Conexión de dispositivos personales	6.2 s	Restringir BYOD, aplicar políticas de validación y monitoreo	Media	90 días
Inventarios tecnológicos	6.2 r, 6.2 i	Realizar inventario periódico, validar licencias de hardware/software	Media	120 días

5.9 Socialización y documentación

Todas las medidas adoptadas han sido recopiladas en un manual interno de Seguridad de la Información, el cual ha sido difundido entre los equipos técnicos y

administrativos de la empresa. Se llevaron a cabo sesiones informativas durante las asambleas generales que se llevan a cabo cada mes para asegurar el adecuado entendimiento y aplicación de los controles establecidos, reconociendo que una documentación precisa es esencial para futuras auditorías BASC y para el proceso de mejora continua.

Las acciones descritas en este capítulo constituyen el primer paso hacia la consolidación de un sistema de seguridad informática en consonancia con el modelo BASC. La selección de medidas se basó en criterios de operatividad simple, bajo costo de implementación y alta eficacia frente a amenazas comunes. Este conjunto integral de soluciones técnicas y administrativas permitirá a la Empresa de Servicios Electrónicos robustecer su infraestructura digital y proteger su cadena logística contra posibles riesgos cibernéticos.

6 Capacitación en Seguridad de la Información para el Personal

La capacitación del recurso humano se erige como un elemento crítico para el éxito de cualquier estrategia de seguridad de la información. Incluso con herramientas tecnológicas avanzadas, la seguridad sigue dependiendo del factor humano: prácticas inseguras, desconocimiento o comportamientos rutinarios inapropiados pueden invalidar controles técnicos y exponer a la organización a incidentes de seguridad. Por eso, la formación debe diseñarse como una intervención continua, práctica y basada en riesgos, con el fin de alinear el comportamiento del personal con los controles establecidos por el Sistema de Gestión en Control y Seguridad (SGCS) BASC y las mejores prácticas internacionales como ISO/IEC 27001. [1][2]

La Norma BASC exige no solo controles técnicos, sino la gestión del factor humano dentro del SGCS: documentación, evidencias de formación, sensibilización sobre amenazas y la demostración de que el personal entiende y aplica los procedimientos de seguridad en su trabajo diario. Integrar un programa de formación sistemático ayuda a cubrir requisitos de políticas, evidencia de implementación y continuidad del control operativo exigidos en auditorías BASC. [3]

ISO/IEC 27001 contempla explícitamente la concientización, la educación y la formación como medidas para mitigar riesgos humanos y mantener la competencia del personal. Por tanto, un programa alineado a BASC debe evidenciar cómo satisface los requisitos de A.7, esto facilita la interoperabilidad entre ambos marcos. [2] [3]

6.1 Propuesta de Capacitación

Se implementará un plan integral de capacitación dirigido a todo el personal de la empresa, con el propósito de fortalecer sus conocimientos y competencias en

materia de seguridad. Este plan busca consolidar una cultura de seguridad sostenida que minimice la probabilidad de incidentes derivados de errores humanos, garantice la correcta aplicación de los controles BASC y asegure la generación de evidencia verificable para auditorías internas y externas. La capacitación incluirá sesiones teóricas y prácticas, orientadas a la comprensión de procedimientos, la identificación de riesgos y la adopción de conductas seguras en cada etapa de la operación, promoviendo así el compromiso individual y colectivo con los estándares internacionales de seguridad.

El programa se estructura en componentes esenciales que garantizan su efectividad y alineación con los estándares BASC:

6.1.1 Diagnóstico inicial

Se realizará una evaluación integral de conocimientos, conductas y riesgos según el rol de cada colaborador. Este diagnóstico incluirá encuestas, simulaciones de phishing y revisión de incidentes históricos, permitiendo identificar brechas y diseñar acciones correctivas específicas.

6.1.2 Plan de contenidos por rol

Se desarrollarán módulos obligatorios adaptados a cada grupo: alta gerencia (gobernanza y gestión de riesgos), personal de TI (administración segura), usuarios operativos (manejo seguro de información y reconocimiento de intentos de phishing), proveedores y personal de planta (procedimientos físicos y control de accesos). Esta segmentación asegura que cada participante reciba formación relevante para sus responsabilidades.

6.1.3 Metodología mixta y práctica

El programa combinará cápsulas de 5 minutos, talleres virtuales, simulaciones de phishing y casos prácticos vinculados a procesos críticos. Esta metodología busca maximizar la retención y aplicación del conocimiento en escenarios reales.

6.1.4 Refuerzo y frecuencia

Se establecerán sensibilizaciones periódicas trimestrales, formaciones obligatorias anuales y refuerzos ad hoc ante cambios en procesos o incidentes relevantes. Este enfoque garantiza la continuidad y actualización de la cultura de seguridad.

6.1.5 Evaluación y métricas

Se implementarán indicadores para medir el impacto del programa: porcentaje de cumplimiento de formación, tasa de clics en simulaciones de phishing, número de incidentes atribuibles a error humano y resultados de encuestas de actitud y conocimiento antes y después de la capacitación.

6.1.6 Evidencia y trazabilidad

Se mantendrán registros electrónicos, listas de asistencia, resultados de simulaciones y reportes de mejora, cumpliendo con los requisitos de auditoría BASC y asegurando la trazabilidad de todas las acciones formativas.

6.2 Diseño didáctico y buenas prácticas

El diseño del programa de capacitación se fundamenta en principios pedagógicos, evidencia empírica y recomendaciones de organismos especializados (SANS, NIST, BASC), asegurando que la formación no solo transmita conocimiento, sino que genere cambios sostenibles en la conducta del personal. A continuación, se detallan las directrices clave:

6.2.1 Entrenamiento regular y simulaciones prácticas

La literatura especializada y los reportes de organismos internacionales coinciden en que la combinación de formación interactiva con simulaciones periódicas es el método más eficaz para reducir la vulnerabilidad frente a amenazas reales.

6.2.1.1 Formación continua y adaptada al rol

El aprendizaje debe ser recurrente y segmentado según las funciones del colaborador, para garantizar relevancia y aplicabilidad.

6.2.1.2 Simulaciones realistas

Las pruebas prácticas, como campañas simuladas de phishing, permiten evaluar la respuesta del personal en condiciones similares a las reales, reforzando la toma de decisiones segura.

6.2.1.3 Prioridad en la práctica sobre la teoría

Aunque los contenidos teóricos son necesarios, el énfasis debe estar en ejercicios prácticos que desarrollen habilidades operativas y pensamiento crítico frente a riesgos.

6.2.1.4 Microlearning y aprendizaje experiencial

El uso de cápsulas cortas y dinámicas interactivas facilita la retención del conocimiento y reduce la fatiga cognitiva.

6.2.2 Medición orientada al comportamiento

La efectividad del programa no debe evaluarse únicamente por la finalización de cursos, sino por la evidencia de cambios en la conducta del personal.

6.2.2.1 Indicadores clave

- Reducción en la tasa de clics en simulaciones de phishing.
- Incremento en reportes proactivos de correos sospechosos.
- Disminución de incidentes atribuibles a error humano.

6.2.2.2 Evaluación pre y post capacitación

Comparar resultados antes y después de la formación permite medir el impacto real y demostrar mejora continua.

6.2.2.3 Valor para auditorías BASC

Los auditores priorizan evidencia verificable de cambio conductual, lo que refuerza la necesidad de métricas orientadas a resultados tangibles.

6.2.3 Apoyo y liderazgo ejecutivo

El compromiso visible de la alta dirección es un factor crítico para la sostenibilidad del programa.

6.2.3.1 Patrocinio institucional

La asignación de recursos y la inclusión del programa en la estrategia corporativa demuestran su relevancia.

6.2.3.2 Comunicación activa del liderazgo

Mensajes claros desde la gerencia refuerzan la importancia de la seguridad y fomentan la adherencia cultural.

6.2.3.3 Modelado de conducta

Cuando los líderes participan en las capacitaciones y cumplen con los estándares, se genera un efecto multiplicador en la organización.

6.2.3.4 Referencias internacionales

Estudios de SANS y NIST confirman que el liderazgo visible es determinante para lograr cambios sostenidos en la cultura organizacional.

6.2.4 Buenas prácticas complementarias

Gamificación: Incorporar dinámicas competitivas y recompensas incrementa la motivación y la participación.

Refuerzo periódico: Sensibilizaciones trimestrales y capacitaciones anuales obligatorias mantienen la atención y actualizan conocimientos frente a nuevas amenazas.

Integración con procesos críticos: Los casos prácticos deben vincularse a operaciones reales de la empresa, asegurando aplicabilidad inmediata.

Trazabilidad y evidencia: Mantener registros electrónicos, listas de asistencia y resultados de simulaciones garantiza cumplimiento normativo y facilita auditorías.

Una vez definidos los criterios de la capacitación, se procede a definir el plan de capacitación del personal.

6.3 Plan de Capacitación del Personal

El plan de capacitación se encuentra dividido en 6 fases y se encuentra alineado a lo establecido en el procedimiento de capacitación y concientización en el Anexo: TI-CCS-PR-05

6.3.1 Fase 0 — Aprobación y gobernanza (0–15 días)

- Aprobación por la dirección, asignación de responsables y presupuesto.
- Inclusión del programa en el SGCS-BASC como control documentado.

6.3.2 Fase 1 — Diagnóstico (15–30 días)

- Encuestas, inventario de formación existente, pruebas de phishing base-line.

6.3.3 Fase 2 — Diseño y contenidos (30–60 días)

- Creación de módulos por rol, calendario, materiales y criterios de evaluación (KPI).

6.3.4 Fase 3 — Ejecución piloto (60–90 días)

- Implementación en un área piloto con Logística, realización de 1 simulación y ajuste.

6.3.5 Fase 4 — Despliegue y seguimiento continuo (desde 90 días)

- Extensión al resto de la organización, calendario de refuerzos trimestrales y reportes de métricas para junta.

6.3.6 Fase 5 — Auditoría y mejora contínua

- Revisión anual, análisis de efectividad y mejoras documentadas para evidenciar conforme a BASC.

Este enfoque asegura que la capacitación no sea un evento aislado, sino un proceso continuo que fortalezca la cultura de seguridad reduzca riesgos humanos y cumpla con los estándares BASC.

El proceso de capacitación se estructuró en módulos concisos con un fuerte enfoque práctico. Los temas principales abordados incluyeron:

- Identificación de correos electrónicos y enlaces sospechosos (phishing).
- Buenas prácticas en la gestión y seguridad de contraseñas.
- Estrategias seguras para proteger información digital en dispositivos como USB, en la nube y en equipos móviles.
- Protocolos básicos para la respuesta ante incidentes cibernéticos.
- Uso responsable de los dispositivos conectados a la red corporativa.

Para facilitar la asimilación de estos conceptos, se recurrió al uso de manuales digitales, presentaciones interactivas y videos educativos, lo que permitió adaptar la formación a diversos niveles de conocimiento del personal (Von Solms & Van Niekerk, 2013).

6.3.7 Modalidad de las capacitaciones

Las sesiones formativas se impartieron en el formato virtual, donde se desarrollaron sesiones asincrónicas a través de la plataforma de capacitación de Microsoft Teams, complementadas con cuestionarios de autoevaluación.

7 Resultados obtenidos

Una vez implementados los controles, se actualiza la matriz de control del SGCS-BASC en donde se determina el cumplimiento del estándar con los controles implementados, esta información se documenta y se envía para la revisión del auditor del capítulo BASC en el que se encuentre registrado la empresa, que para este caso es BASC Azuay.

Tabla 16. Matriz de Control del SGCS-BASC de la Empresa de Servicios Electrónicos Actualizada

REQ.	PARAMETROS	RESPONSABLE	PROCESO	ESTADO	ANOTACIONES
6	SEGURIDAD DE LA INFORMACIÓN				
6,1	Generalidades				Procedimiento de Seguridad TI
6.1 a	Gestionar y proteger información y tecnología	Analista TI	Seguridad TI	Si	Política de Seguridad de TI
6.1 b	Salvaguardar información confidencial	Analista TI	Seguridad TI	Si	Matriz de Criticidad
6.1 c	Proteger infraestructura tecnológica	Analista TI	Seguridad TI	Si	TI-SEG-POL-04
6,2	Ciberseguridad y las tecnologías de información				
6.2 a	Criterios de seguridad (Proteger y recuperar)	Analista TI	Seguridad TI	SI	TI-BCP-DRP-01
6.2 b	Identificar partes interesadas	Analista TI	Seguridad TI	Si	Política de Seguridad
6.2 c	Comunicar amenazas de ciberseguridad	Analista TI	Seguridad TI	Si	Política de Seguridad
6.2 d	Clasificar información según criticidad	Analista TI	Seguridad TI	Si	TI-INF-POL-02
6.2 e	Cuentas asignadas para cada usuario	Analista TI	Seguridad TI	SI	TI-SEG-POL-04
6.2 f	Limitar acceso y permisos (Funciones)	Analista TI	Seguridad TI	SI	TI-GAP-POL-01
6.2 g	Eliminar acceso al terminar contrato	Analista TI	Seguridad TI	Si	Informe de retiro de accesos
6.2 h	Impedir instalación software no autorizado	Analista TI	Seguridad TI	Si	Matriz de Seguridad TI
6.2 i	Licencia de hardware y software	Analista TI	Seguridad TI	SI	TI-LAC-POL-01
6.2 j	Realizar copia de seguridad	Analista TI	Seguridad TI	Si	Política de Seguridad
6.2 k	Registro actualizado de usuario	Analista TI	Seguridad TI	Si	Listado de usuarios
6.2 l	Cerrar/Bloquear equipos desatendidos	Analista TI	Seguridad TI	Si	Política de Seguridad
6.2 m	Evaluar infraestructura tecnológica (Anual)	Analista TI	Seguridad TI	Si	Política de Seguridad
6.2 n	Identificar y reportar accesos no autorizados	Analista TI	Seguridad TI	Si	Política de Seguridad
6.2 o	Revisar políticas de ciberseguridad	Analista TI	Seguridad TI	Si	Política de Seguridad
6.2 p	Emplear tecnología segura (VPN)	Analista TI	Seguridad TI	Si	Autentificador multifactor
6.2 q	Evitar acceso remoto a la información	Analista TI	Seguridad TI	Si	Política de Seguridad
6.2 r	Realizar inventario tecnológico	Analista TI	Seguridad TI	SI	TI-GAT-POL-01
6.2 s	Restringir conexión de dispositivos personales	Analista TI	Seguridad TI	No	TI-BCP-POL-01
6.2 t	Evaluar políticas de ciberseguridad	Analista TI	Seguridad TI	Si	Política de Seguridad
6.2 u	Realizar simulacros y ejercicios de tecnología	Analista TI	Seguridad TI	Si	TI-CCS-POL-05
6.2 v	Controles para super usuarios	Analista TI	Seguridad TI	No	TI-GSU-POL-01
RESULTADOS GLOBALES=========>				100%	

Durante el proceso de auditoría externa realizado por la entidad certificadora, el auditor seleccionó 5 controles sobre los cuales se evaluó el cumplimiento y que se encuentre alineado a la documentación presentada y de los que no se presentaron observaciones, indicando un cumplimiento total con el estándar.

Ahora bien, es necesario también evaluar los resultados considerando la implementación de los controles y las capacitaciones al personal de las diferentes áreas de la empresa.

Como punto inicial, se analiza nuevamente la matriz de riesgos considerando nuevos valores de probabilidad e impacto, posterior a la implementación de los controles y se valida el efecto de estos sobre los riesgos.

Tabla 17. Matriz de Probabilidad e Impacto de los Riesgos con los Controles Implementados en el Empresa de Servicios Electrónicos

Riesgo	Probabilidad	Impacto	Justificación
1. Ubicación del datacenter sin medidas de seguridad adecuadas.	2	4	Poco improbable que ocurra, el impacto es crítico debido a la exposición de la infraestructura física.
2. Ausencia de planes de acción o contingencia en caso de pérdida de información o daño de servidores virtualizados.	3	3	Probabilidad moderada, el impacto se reduce a alto porque en un determinado evento, se puede reaccionar adecuadamente.
3. Falta de categorización de la información y control de acceso por cargo.	2	3	Poco improbable que ocurra con las políticas claras; el impacto es moderado debido al control sobre datos sensibles.
4. Uso compartido de credenciales sin controles específicos.	1	3	Muy improbable y que cada usuario usa sus credenciales; el impacto es moderado ya que se puede rastrear accesos y proteger la información.
5. Sin control del número licencias utilizadas, ni fechas de caducidad.	1	3	Muy improbable; el impacto alto, porque si bien se lleva el control de caducidad de las licencias usadas en las operaciones de la empresa, queda sujeto a control humano.
6. Ausencia de mecanismos para limitar el acceso a sistemas según cargo.	2	2	Poco improbable, existe política de acceso claras; el impacto es moderado, la información es accesible únicamente por quienes la necesitan.

7. Falta de inventarios periódicos y revisión de estados de infraestructura tecnológica.	2	1	Poco improbable, se puede detectar fallos en la infraestructura; impacto bajo al tener revisiones periódicas.
8. Control deficiente sobre la conexión de dispositivos personales.	1	2	Muy improbable, con controles estrictos; el impacto es moderado por el registro de dispositivos personales utilizados.
9. Ausencia de plan de simulacros y capacitación para el personal.	2	3	Poco improbable porque depende del factor humano; el impacto es alto.
10. Dependencia excesiva del personal técnico sin controles ni respaldo documental.	2	2	Poco improbable, se reqiere mantener los procedimientos documentados; el impacto es moderado por mantener información crítica respaldada.

De la cual se extrae la Matriz de Riesgos Actualizada considerando los controles implementados, donde se observa que la probabilidad/impacto de los riesgos analizados se reduce, lo que indica que los riesgos han sido mitigados y por lo tanto, la organización se encuentra protegida ante cualquiera de estas eventualidades.

Tabla 18. Matriz de Riesgos Actualizad de la Empresa de Servicios Electrónicos

Probabilidad	**Impacto**				
	Bajo (1)	**Moderado (2)**	**Alto (3)**	**Crítico (4)**	**Muy Crítico (5)**
Muy Improbable (1)		Riesgo 7 / Riesgo 8	Riesgo 4 / Riesgo 5		
Poco Improbable (2)		Riesgo 6 / Riesgo 10	Riesgo 3 / Riesgo 9	Riesgo 1	
Moderado (3)			Riesgo 2		
Probable (4)					
Muy Probable (5)					

Una vez analizado los controles y su efecto en la organización, se procede con el análisis de las capacitaciones del personal. Tras la esta implementación, se llevó a cabo una evaluación comparativa entre el Diagnostico Inicial y los datos recopilados después del proceso. Los resultados evidenciaron:

- El número de correos de phishing abiertos se redujo de un 100% a un 54% y la interacción del 3% a 0% lo que se puede interpretar como un incremento del 47% en la capacidad para identificar amenazas comunes respecto a la evaluación de control.
- Se detecta además un incremento del 65% en el índice de reportes de conductas anómalas.
- Un fortalecimiento de las contraseñas al implementar políticas que impiden el uso de contraseñas débiles o repetitivas.
- La mejora el desempeño en la respuesta a incidentes pasando de una evaluación promedio de 59% a un promedio de 73%.
- Se reduce el número de dispositivos no registrados conectados a la red corporativa de 21 a 8, los cuales se mantienen mediante solicitud de acceso y por cortos periodos de tiempo.
- El personal mantiene la reserva de sus credenciales, no se detecta personal compartiendo credenciales de acceso.

Estos resultados reflejan una mejora sustancial en la cultura tecnológica de los miembros de la organización, presentando la base para avanzar en la protección integral de la información.

8 Conclusiones

- Los controles establecidos por el estándar BASC V6 demuestran tener un enfoque muy útil para empresas que deseen proteger sus operaciones en todas sus áreas y no centrarse en un solo apartado, aunque no es tan específica como un estándar especializado, sus controles han demostrado ser efectivos en el ámbito de Seguridad de la Información reduciendo los riesgos y probabilidad de ocurrencia y mejorando la respuesta del personal ante los riesgos que pueden enfrentar.
- Considerando el entorno sobre el que la Empresa de Servicios Electrónicos desarrolla sus operaciones y el giro de negocio en el que se desenvuelve, es indispensable establecer mecanismos que le permitan mantener un control estricto sobre su cadena de logística y sus operaciones comerciales, mismos que están apoyados sobre una infraestructura tecnológica, en este contexto, la Normativa BASC V6 contiene mecanismos integrales para la protección de esta infraestructura y que tiene que ser complementada con estándares internacionales especializados en Seguridad de la Información como la ISO 27001 para robustecer los controles y así contribuir a generar una empresa más resiliente ante los efectos de la explotación de sus vulnerabilidades.
- Si bien en BASC V6 se establece un listado claro de controles mínimos se deben cumplir en el apartado de Seguridad de la Información para asegurar que la empresa pueda resolver correctamente eventos de este tipo, adicionalmente fomenta la capacitación al personal como parte del proceso de mejora continua para desarrollar una cultura tecnológica adecuada, misma que las empresas deben tener como objetivo principal y, para su cumplimiento, se debe sumar el compromiso de todos los niveles que componen la organización.
- El proceso periódico de auditorías, es el otro componente de la mejora continua que requiere BASC V6, en este se verifica, mediante el control documental, que las empresas realicen las revisiones de sus políticas y procesos, de esta forma, siempre estarán actualizados y alineados, no solo a los requisitos que establece la norma, sino también a los objetivos institucionales que se fija la organización

9 Referencias

Echeverría, J. A., Torres-Sainz, R. I., María Pérez-Vallejo, L. I., Alberto Trinchet-Varela, C. I., Pérez-Rodríguez, R. I., & de la Rosa III, J. E. (2024). *Criterios de criticidad y complejidad para la toma de decisiones de mantenimiento: una revisión de la literatura*. https://ingenieriamecanica.cujae.edu.cu

ARCOTEL. (2024). *Reporte Anual de Incidentes de Seguridad 2023*.

Bank, I. A. D., & States, O. of A. (2016). Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? *Cybersecurity: Are We Ready in Latin America and the Caribbean?* https://doi.org/10.18235/0006517

BASC Ecuador Capítulo Cuenca. (2025). *Auditorias*. https://basc-azuay.org/index.php/informacion-juridica/auditorias

BASC Global. (2025). *Proceso de certificación | Business Alliance*. https://www.bascglobal.org/es/certificacion/proceso-de-certificacion

CNCS. (2020). *Guía de Controles Críticos de Ciberseguridad*.

Consejo Nacional de Evaluación de la Política de Desarrollo Social. (2025). Guía rápida para la construcción de la Matriz de Indicadores para Resultados. *CONEVAL*. http://www.coneval.org.mx

Consejo Profesional de Ciencias Económicas. (2023). *Guía Para la Elaboración de Matrices de Riesgo*. www.consejo.org.ar

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice 2022 47:3*, *47*(3), 698–736. https://doi.org/10.1057/S41288-022-00266-6

D. H. Stamatis. (2003). *Failure Mode and Effect Analysis: FMEA from Theory to Execution*. 1–65. https://books.google.com/books/about/Failure_Mode_and_Effect_Analysis.html?hl=es&id=TTxI8jbTkVwC

Dal Cin, P., & Jurgens, J. (2023). *Global Cybersecurity Outlook 2023*.

Díaz del Castillo Náder, E., & Caballero Olivares, J. E. (2020). *Herramientas y técnicas fundamentales del PMBOKv6 para recolección análisis y representación de datos en la toma de decisiones gerenciales*. Universidad Nacional Abierta y a Distancia.

Díaz, R. M. (2021). Estado de la ciberseguridad en la logística de América Latina y el Caribe. *CEPAL - Serie Desarrollo Productivo N° 228*. www.cepal.org/apps

Dirección General De Desarrollo Institucional Y Aseguramiento De La Calidad. (2025). Manual De Elaboración De La Matriz FODA Para El Plan De Desarrollo Estratégico. *Universidad de Valparaíso*.

ENISA. (2021). *Cybersecurity guide for SMEs 12 STEPS TO SECURING YOUR BUSINESS*. EUROPEAN UNION AGENCY FOR CYBERSECURITY.

Guerrero Aguiar, M., Medina León, A., & Nogueira Rivera, D. (2020). *Procedimiento de gestión de riesgos como apoyo a la toma de decisiones*. http://orcid.org/0000-0002-0198-852X

IEEE Communications Society. (n.d.). *Balancing Privacy and Security in the Digital Age - IEEE Digital Privacy*. Retrieved November 19, 2025, from https://digitalprivacy.ieee.org/publications/topics/balancing-privacy-and-security-in-the-digital-age/

International Organization for Standardization. (2018). *Risk management-Guidelines*.

ISO/IEC. (2022). *ISO/IEC 27005:2022 - Guidance on managing information security risks*. https://www.iso.org/es/contents/data/standard/08/05/80585.html

ISO/IEC. (2022a). *ISO/IEC 27001:2022 - Information security management systems*. https://www.iso.org/standard/27001

ISO/IEC. (2022b). *ISO/IEC 27001:2022(en), Information security, cybersecurity and privacy protection*. https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27001:ed-3:v1:en

ISO/IEC. (2022c). *ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls*. https://www.iso.org/es/contents/data/standard/07/56/75652.html

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal. *International Journal of Information Security 2025 24:3*, *24*(3), 119-. https://doi.org/10.1007/S10207-025-01032-0

LOPDP. (2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*. www.lexis.com.ec

Mamami, R. G. R., Argollo, R. R. L., & Ancco, R. C. (2023). Política informática y la gestión de la seguridad de la información en base a la norma ISO 27001. *Innovación y Software*, *4*(1), 96–106. https://doi.org/10.20511/PYR2020.V8N3.786

Mantilla Rivera, F. (2024). Análisis crítico de la gestión de Seguridad y Salud Ocupacional, en una entidad pública del Distrito Metropolitano de Quito, 2023 – 2024. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades*, *5*(4). https://doi.org/10.56712/latam.v5i4.2457

Méndez Morales, K. A., & Yupa Cabadiana, M. M. (2019). *Estrategia para la implementación de Sistema Business Alliance For Secure Commerce BASC para la empresa Servireefertransport S.A.* (B. I. Delgado Litardo, Ed.; Issue 2019). Universidad de Guayaquil Facultad de Ciencias Administrativas. http://repositorio.ug.edu.ec/handle/redug/45610

Mora Navarro, Ó. E. (2022). Gestión de riesgos: un desafío para las organizaciones. *Administración & Desarrollo*, *52*(1), 4–19. https://doi.org/10.22431/25005227.vol52n1.1

Mora Navarro, O. E. (2022). Gestión de riesgos: un desafío para las organizaciones. *Administración & Desarrollo, ISSN-e 0120-3754, Vol. 52, No. 1, 2022, Págs. 4-19*, *52*(1), 4–19. https://doi.org/10.22431/25005227.vol52n1.1

Oswaldo, J., & Reina, F. (2022). The impact of comprehensive risk management in the current contex. *South Florida Journal of Development*, 2731–2748. https://doi.org/10.46932/sfjdv3n2-091

Restrepo-Olarte, A. C., & Cogollo-Flórez, J. M. (2021). *Metodología multicriterio para la identificación y clasificación de partes interesadas pertinentes*. https://doi.org/10.15665/dem.v19i2.2688

Romero, M. T. (n.d.). *Diseño y aplicación de un Análisis de Criticidad, interpretación de resultados y planes de acción sugeridos*.

Salgado Romero, E. (2025). PROPUESTA METODOLÓGICA PARA IMPLEMENTAR UN PROCEDIMIENTO DE ACCIONES CORRECTIVAS EN UNA EMPRESA DE

CONSULTORÍA DE ACUERDO A LA NORMA ISO 9001:2015. *Universidad Nacional Autónoma de México*.

Sargiotis, D. (2024). Data Security and Privacy: Protecting Sensitive Information. *Data Governance*, 217–245. https://doi.org/10.1007/978-3-031-67268-2_6

UDAX. (2024, December 30). Gestión de la Privacidad y Protección de Datos en las Organizaciones: Un Enfoque Integral. *Revista Digital Experiencia UDAX*. https://udax.edu.mx/experiencia/empresas-y-negocios/gestion-de-la-privacidad-y-proteccion-de-datos-en-las-organizaciones-un-enfoque-integral

WBO. (2022). *ESTÁNDAR INTERNACIONAL DE SEGURIDAD BASC 6.0.1*.

World BASC Organization. (2022). *NORMA INTERNACIONAL BASC*.

World BASC Organization. (2022). *GUIAS DE IMPLEMENTACION VERSION 2022 ESPAÑOL*.

10 ANEXOS

A. Anexo: TI-PIC-PR-01

Plan de Implementación de Controles BASC

Código Documental	TI-PIC-PR-01
Versión	1.0
Fecha	03/12/2025
Responsables	Analista TI / Representantes SGCS-BASC / Analista de Procesos

1. Introducción

La gestión de riesgos constituye un componente esencial en los sistemas de control y aseguramiento de la cadena logística, especialmente bajo estándares internacionales como BASC (Business Alliance for Secure Commerce), cuyo objetivo es prevenir actividades ilícitas y garantizar la seguridad en el comercio internacional. En este contexto, la matriz de probabilidad e impacto se presenta como una herramienta metodológica clave para la evaluación cualitativa y cuantitativa de riesgos, permitiendo priorizar acciones correctivas y asignar recursos de manera eficiente.

Según el PMBOK® Guide (6ª edición), la matriz de probabilidad e impacto es una cuadrícula que relaciona la probabilidad de ocurrencia de un riesgo con el impacto que este tendría sobre los objetivos del proyecto u organización, en caso de materializarse. Esta técnica facilita la clasificación de riesgos en niveles de criticidad (bajo, medio, alto), lo que permite orientar la toma de decisiones hacia aquellos riesgos que requieren atención inmediata (Project Management Institute, 2017).

En el marco BASC, la aplicación de esta matriz se fundamenta en la necesidad de mitigar vulnerabilidades en la cadena de suministro, considerando factores como la ubicación física de instalaciones, controles de acceso, planes de contingencia y políticas de seguridad informática.

2. Referencias:

Project Management Institute. (2017). Guía de los Fundamentos para la Dirección de Proyectos (PMBOK® Guide).
Miles, J. (2021). Gestión de Riesgos: Un aporte práctico. Montevideo: Modum Srl.
Kerzner, H. (2013). Project Management: A Systems Approach to Planning, Scheduling, and Controlling. Wiley.

3. Configuración de la matriz de probabilidad e impacto

La matriz de probabilidad e impacto se estructura en una cuadrícula donde las filas representan el nivel de impacto y las columnas indican la probabilidad de ocurrencia. Cada celda refleja el nivel de riesgo resultante, calculado mediante la fórmula: Nivel de Riesgo = Probabilidad × Impacto.

Las escalas utilizadas suelen ser numéricas (1 a 5) o cualitativas, definidas según el contexto organizacional. Por ejemplo: Probabilidad: 1 (rara) a 5 (muy probable); Impacto: 1 (mínimo) a 5 (catastrófico). La norma BASC recomienda establecer criterios claros para cada nivel, considerando factores como la frecuencia histórica, vulnerabilidades del proceso y consecuencias económicas, operativas o reputacionales.

4. Plan de Implementación de Controles

El plan se basa en la priorización de riesgos según la matriz presentada, atendiendo primero aquellos con criticidad alta (≥20). Se definen acciones específicas alineadas con los criterios BASC (6.1 y 6.2), responsables y plazos.

Riesgo Crítico	Control BASC	Acción Específica	Prioridad	Plazo

Uso compartido de credenciales	6.2 e, 6.2 f, 6.2 v	Implementar autenticación individual, MFA, prohibir credenciales compartidas	Alta	30 días
Ausencia de planes de contingencia	6.2 a, 6.2 u	Diseñar plan de recuperación ante desastres, realizar simulacros	Alta	45 días
Ubicación del datacenter sin seguridad	6.1 c	Instalar sistemas de control físico	Alta	60 días
Falta de categorización de información	6.2 a	Clasificar información según criticidad, definir políticas de acceso	Alta	60 días
Ausencia de mecanismos para limitar acceso	6.2 f	Implementar RBAC (Role-Based Access Control)	Alta	60 días
Dependencia excesiva del personal técnico	6.2 v	Documentar procedimientos críticos, crear cuentas individuales	Media	90 días
Conexión de dispositivos personales	6.2 s	Restringir BYOD, aplicar políticas de validación y monitoreo	Media	90 días
Inventarios tecnológicos	6.2 r, 6.2 i	Realizar inventario periódico, validar licencias de hardware/software	Media	120 días

5. Conclusiones

La implementación de controles priorizados según la matriz de riesgos permite reducir la exposición a amenazas críticas, garantizar la continuidad operativa y cumplir con los estándares BASC. Se recomienda mantener un ciclo de mejora continua mediante auditorías y simulacros periódicos.

B. Anexo: TI-SEG-MN-01

MANUAL INTERNO DE SEGURIDAD DE LA INFORMACIÓN

Código Documental	TI-SEG-MN-01
Versión	1.0
Fecha	03/12/2025
Responsables	Área TI / Encargados BASC / Encargado de Procesos

1. Tabla de Contenido

2. Glosario y Definiciones

MFA (Autenticación Multifactor): mecanismo que requiere más de un factor para autenticar a un usuario.
RTO (Recovery Time Objective): tiempo máximo permitido para restaurar un servicio tras una interrupción.
RPO (Recovery Point Objective): cantidad máxima de datos que se pueden perder medida en tiempo.
DLP (Data Loss Prevention): herramientas y procesos para evitar la pérdida de datos.

Hardening: proceso de asegurar un sistema reduciendo vulnerabilidades.
Criticidad: nivel de importancia de un activo o sistema para la operación.

1. Introducción

El presente manual consolida el sistema interno de seguridad de la información de la organización y establece directrices, procedimientos, controles y evidencias requeridas para la certificación BASC, en armonía con la Ley Orgánica de Protección de Datos Personales. Su aplicación es obligatoria para todo el personal, contratistas y terceros que accedan a activos de información y servicios tecnológicos. El manual integra políticas y procesos vigentes y define una estructura única para su gobierno, operación y mejora continua.

2. Marco Normativo y Alcance

Este manual establece el sistema interno de seguridad de la información de la organización, conforme a la Norma BASC V (Versión 6 – 2022) y a la Ley Orgánica de Protección de Datos Personales (LOPDP) vigente en Ecuador, incluyendo su reglamentación complementaria. Se aplica a todos los procesos, sistemas y activos de información, digitales y físicos, administrados por el Área de TI, los Encargados BASC y el Encargado de Procesos.

3. Gobierno de Seguridad y Roles

La gobernanza del sistema recae en la Gerencia General, el Área de Tecnologías de la Información, los Responsables de Sistemas, los Custodios de Activos, el Encargado de Procesos y los Representantes del SGCS BASC. La Gerencia aprueba políticas y asigna recursos; TI lidera la implementación técnica, supervisa controles, ejecuta respaldos y gestiona incidentes; los Responsables de Sistemas validan criticidad, accesos y cambios; los Custodios aseguran el uso adecuado de los activos; el Encargado de Procesos mantiene el control documental, versiones y evidencias; los Representantes BASC verifican cumplimiento, aprueban excepciones y coordinan auditorías.

4. Políticas

4.1.TI-SEG-POL-04 Política de Seguridad Tecnológica

Establece los principios de confidencialidad, integridad, disponibilidad y capacidad de recuperación y fija lineamientos para gestión de activos, protección de sistemas, control de accesos, continuidad del negocio, gestión de cambios, monitoreo y auditoría.

4.2.TI-GAT-POL-01 Política de Gestión de Activos Tecnológicos

Exige inventario oficial, asignación de custodios, clasificación por criticidad, uso aceptable, protección y gestión del ciclo de vida desde adquisición hasta baja definitiva.

4.3. TI-LAC-POL-01 Política de Licenciamiento y Actualización

Garantiza el uso de hardware y software licenciados, con registro de licencias, verificación de vigencia y aplicación oportuna de parches y actualizaciones.

4.4. TI-GAP-POL-01 La Política de Gestión de Accesos y Privilegios

Determina que los accesos se otorguen por rol conforme al principio de mínimos privilegios, con segregación de funciones, revisión periódica y trazabilidad; establece autenticación multifactor en sistemas críticos y la caducidad de contraseñas en períodos regulares con parámetros mínimos de complejidad (al menos doce caracteres con mayúsculas, minúsculas, símbolos y números, sin reutilización del historial cuando el sistema lo permita).

4.5. TI-INF-POL-02 Política de Clasificación de Información y Políticas de Acceso

Define los niveles Crítico, Confidencial y Público y dispone controles organizativos y técnicos para asegurar la protección requerida por la LOPDP y BASC.

4.6. TI-GSU-POL-01 Política de Gestión de Superusuarios

Regula la administración de cuentas privilegiadas y la continuidad temporal de credenciales únicamente bajo justificación operativa y autorización formal, con autenticación robusta, monitoreo y trazabilidad.

4.7. TI-BCP-POL-01 Política de Control de Dispositivos Externos

Restringe el uso de dispositivos personales y periféricos no corporativos y exige controles técnicos para impedir conexiones no autorizadas, permitiendo excepciones documentadas y aprobadas.

4.8. TI-SIM-POL-01 Política de Simulacros y Ejercicios

Dispone la planificación anual de ejercicios de respuesta a incidentes, recuperación ante desastres, pérdida de información, interrupción de servicios críticos e ingeniería social, con registro de resultados y acciones de mejora.

5. Procedimientos

5.1. TI-GSU-PR-01 Procedimiento de Control a Superusuarios y Continuidad de Credenciales

Detalla la gestión segura de cuentas privilegiadas, incluyendo inventario y clasificación, validación de necesidad, autorización formal, implementación de controles de autenticación, rotación y auditoría, monitoreo y reporte y la activación de contingencia para preservación temporal de credenciales con registro de motivos, cuentas afectadas, controles adicionales y revocación inmediata al cierre del evento, seguido de informe post-incidente.

5.2. TI-INF-PR-02 Proceso de Clasificación de Información y Gestión de Accesos

Detalla el flujo para inventario, evaluación de criticidad, asignación de nivel, definición de políticas de acceso, implementación de controles (MFA, cifrado), monitoreo y revisión periódica.

5.3. TI-GSU-PR-01-A Procedimiento de Contingencia de Credenciales

Describe la activación del plan, la contención inicial, el mantenimiento de la operativa mínima y la restauración priorizada conforme a la matriz de criticidad y a los objetivos de RTO y RPO, con verificación de integridad, pruebas funcionales y certificación de propietarios antes del retorno a producción; incluye pruebas anuales o cuando existan cambios significativos y revisión anual.

5.4. TI-BCP-PR-01 Proceso de Respaldos y Restauración.

Define la estrategia de respaldo según criticidad, el almacenamiento seguro en ubicaciones independientes con cifrado y acceso restringido, la ejecución con registros verificables, las pruebas periódicas de restauración y la documentación de resultados para revisión por la dirección.

5.5. TI-GAT-PR-01 Proceso de Baja y Eliminación Segura de Equipos.

Regula solicitud y aprobación de baja, respaldo de información, eliminación segura mediante sobreescritura, formateo seguro o destrucción física documentada, actualización del inventario y disposición final conforme a gestor ambiental, con acta de baja y evidencias.

5.6. TI-BCP-PR-01 Procedimiento de Continuidad Operativa y Recuperación Ante Desastres

Establecer las actividades necesarias para asegurar la continuidad de los servicios tecnológicos y la recuperación oportuna de los sistemas de información en caso de interrupciones, incidentes mayores, desastres u otros eventos que comprometan la operación

6. Controles Técnicos y Organizativos

6.1. TI-SEG-CRS-01 Criterios de seguridad para sistemas de TI

Se establecen controles generales para todos los sistemas, como protección antimalware, políticas de contraseñas, parcheo periódico, copias de seguridad, registro y gestión de incidentes y respaldo documental en inventario.

Para sistemas de alta criticidad se exige autenticación multifactor, cifrado de datos en tránsito y reposo, segmentación y aislamiento de red, endurecimiento obligatorio, monitoreo continuo con alertas, parámetros de continuidad con RTO y RPO estrictos, pruebas semestrales de recuperación, copias de seguridad diarias en ubicación externa y retención de logs de auditoría por al menos doce meses con revisión mensual.
Para sistemas de criticidad media se requiere cifrado en tránsito, aplicación oportuna de parches, hardening básico, RTO y RPO moderados y revisión trimestral de registros.
Para sistemas de baja criticidad se mantiene protección mínima, esquema de acceso por roles y respaldos semanales.
Se incluyen controles específicos para servidores, aplicaciones, bases de datos, equipos de red y servicios en nube, con inventario técnico, restricciones de puertos y servicios, control de versiones y pruebas de seguridad antes de cambios mayores, segmentación por VLAN, configuración segura respaldada y evaluación de proveedores con cifrado y MFA obligatorio.

7. Matrices y Registros

7.1. TI-INF-AN-03 Inventario y Clasificación de la Información

La matriz centraliza el inventario de la información de la empresa y su clasificación. Se mantiene como documento controlado independiente y se revisa Periodicamente. A continuación, se incluyen activos representativos:

Matriz de Inventario y Clasificación de la Información						
Activo de Información	Tipo	Formato	Ubicación	Responsable	Criticidad	Controles
Reportes internos Power BI	Operativa	Digital	Power BI Cloud	Área TI	Confidencial	MFA, acceso por rol
Reportes clientes Power BI	Operativa	Digital	Power BI Cloud	Área TI	Confidencial	MFA, acceso por rol
Bases de datos	Personal/Financiera	Digital	Servidor local	Área TI	Crítico	Cifrado, MFA, backup
Políticas y procesos	Documentación	Digital	SharePoint	Encargado de Procesos	Confidencial	Permisos, versionado
Respaldos empleados cesantes	Personal	Digital	NAS	Área TI	Crítico	Cifrado, acceso restringido
Correos electrónicos	Personal/Operativa	Digital	Office 365	Área TI	Confidencial	MFA, monitoreo
ERP (facturación y compras)	Financiera	Digital	Servidor local	Área TI	Crítico	Cifrado, acceso por rol
Contratos de arrendamiento clientes	Legal	Físico/Digital	Archivo/Teams	Encargado de Procesos	Confidencial	Control físico, permisos
Contratos empleados y estatutos	Legal	Físico	Archivo físico	Encargado de Procesos	Confidencial	Control físico
Guías de remisión	Operativa/Logística	Físico/Digital	Archivo/ERP	Encargado de Procesos	Confidencial	Permisos, control físico

Actas de entrega y asignación de equipos	Activos TI	Físico/Digital	Archivo/SharePoint	Área TI	Confidencial	Permisos, control físico
Archivo maestro de credenciales	Accesos privilegiados	Digital	Repositorio cifrado	Analista TI	Crítico	Cifrado, MFA, bitácora

7.2. TI-CRC-AN-03 Matriz de Criticidad de Cargos

Se establece la Matriz de Criticidad de Cargos, con referencia en la categoriza a cada cargo de acuerdo la criticidad de la información a la que necesita acceder.

Matriz de Criticidad de Cargos						
Cargo	**Criticidad**	**Tipo de Información Permitida**	**Nivel de Acceso**	**Sistemas Autorizados**	**Restricciones**	**Justificación**
Gerencia	**Alta**	Información estratégica, financiera	Lectura / Aprobación	ERP, CRM, Documentación de estrategia	Sin acceso técnico	Información para decisiones, administración técnica limitada
Presidencia	**Alta**	Información financiera, legal	Lectura / Aprobación	Información Legal y Financiera, ERP	Sin acceso técnico	Información para control administrativo
Servicios	**Alta**	Información estratégica y técnica	Lectura / Escritura	Documentación Estratégica, documentación técnica	Sin acceso técnico	Gestiona las decisiones desde Gerencia hacia TI y Arriendos
Analista TI	**Alta**	Infraestructura, servidores, redes	Administrador	Servidores, AD, Backups, Seguridad	Auditoría obligatoria	Administra la infraestructura crítica
Desarrollador TI	**Alta**	ERP, Activos	Super usuario	Aplicación ERP, Bases de Datos	Auditoría obligatoria	Administra la infraestructura crítica
Contabilidad	Media	Información contable, tributaria	Lectura / Escritura	ERP Financiero	Sin acceso técnico	Maneja datos financieros críticos
Recursos Humanos	Media	Datos personales, nómina	Lectura / Escritura	Sistema RRHH	Sin acceso financiero ni técnico	Maneja información sensible del personal
Logística	Alta	Información de Cadena de suministros	Lectura / Escritura	Movimientos de inventario, ERP módulos operativos	Sin acceso financiero ni técnico	Maneja el abastecimiento y distribución del inventario
Jefes de Área	Media	Información operativa	Lectura / Escritura en su área	CRM, ERP Módulos de Facturación, Activos	Sin acceso a datos críticos	Requiere supervisión operativa
Departamento técnico	Baja	Datos básicos para funciones	Lectura	Sistema operativo correspondiente	Sin acceso confidencial	Acceso mínimo necesario
Arriendos	Media	Documentos internos	Lectura / Escritura limitada	ERP Módulos de Facturación, Activos, Mesa de Ayuda Clientes	Sin acceso financiero	Acceso básico para tareas administrativas
Recepción	Baja	Información operativa	Lectura / Escritura	Activos, Mesa de Ayuda Interna	Sin acceso financiero ni técnico	Acceso básico para tareas administrativas

Despachos	Baja	Información operativa	Lectura	Solo red empresarial	Sin acceso confidencial	Acceso mínimo necesario
Auxiliar de Limpieza	Baja	Politicas generales	Lectura	Solo red empresarial	Sin acceso confidencial	Acceso mínimo necesario
Visitantes / Proveedores	Nulo	Ninguna	Ninguna	Solo red invitados	Sin acceso corporativo	Prevención de riesgos externos

7.3. TI-CRC-AN-04: Niveles de Criticidad Según cada Cargo

La matriz permite determinar los coeficientes, con base en los accesos que requiere el usuario para poder realizar sus funciones, sobre los cuales se determina la criticidad del cargo.

Matriz de Evaluación de Criterios por Cargo							
Cargo	**Infor. sensible**	**Sistemas críticos**	**Privilegios técnicos**	**Impacto operación**	**Acceso físico áreas críticas**	**Cadena logística**	**Total**
Gerencia	3	3	1	3	1	3	14
Presidencia	3	3	0	3	1	2	12
Servicios	3	3	2	2	3	1	14
Analista TI	3	3	3	3	3	2	17
Desarrollador TI	3	3	2	3	1	3	15
Contabilidad	3	2	0	3	0	2	10
Recursos Humanos	2	2	0	2	0	1	7
Logística	2	2	0	3	1	3	11
Jefes de Área	2	2	0	2	0	1	7
Departamento técnico	0	0	0	1	2	0	3
Arriendos	2	2	0	2	0	1	7
Recepción	0	0	0	1	2	1	4
Despachos	0	0	0	1	0	3	4
Auxiliar de Limpieza	0	0	0	0	2	0	2

7.4. TI-BCK-AN-03 Matriz de Frecuencia y Criticidad de Respaldo

Esta matriz permite establecer la frecuencia con la que se tienen que realizar los respaldos considerando la criticidad del sistema.

Matriz Única de Frecuencia y Criticidad de Respaldo				
Categoría	**Activo / Sistema**	**Responsable**	**Criticidad**	**Frecuencia**
Servidor	VMware ESXi 7.0	Analista TI	Crítico	Diario
Servidor	VMware ESXi 7.1	Analista TI	Crítico	Diario
Servidor	Windows Server 2019	Analista TI	Crítico	Diario
Servidor	NAS Synology	Analista TI	Alto	Semanal
VoIP	UCM3626	Analista TI	Medio	Semanal
VoIP	Teléfonos IP Grandstream	Analista TI	Bajo	Mensual
Seguridad	NVR Hikvision	Analista TI	Crítico	Diario
Seguridad	Cámaras IP Hikvision	Analista TI	Alto	Semanal
Seguridad	Reloj Biométrico ZKTeco	Proveedor	Bajo	Mensual
Aplicación	Microsoft 365	Analista TI	Crítico	Diario
Aplicación	KPAX	Analista TI	Bajo	Mensual
Software	VMware vCenter	Analista TI	Crítico	Diario
Software	ESET	Analista TI	Crítico	Diario
Software	PaperCut	Analista TI	Bajo	Mensual
Software	Perseo	Desarrollador TI	Crítico	Diario
Software	Veeam Backup	Analista TI	Crítico	Diario

Software	Directorio Activo	Analista TI	Crítico	Diario
Software	Directorio Activo 2	Analista TI	Alto	Semanal
Software	GLPI	Analista TI	Bajo	Mensual
Software	Service Desk	Analista TI	Medio	Semanal
Software	Base de Datos	Desarrollador TI	Medio	Semanal
Software	Sistema de Activos	Desarrollador TI	Crítico	Diario
Software	OCS Inventory	Analista TI	Crítico	Diario
Red	Switch L3 Core	Analista TI	Medio	Semanal
Red	Switch Servidores	Analista TI	Bajo	Mensual
Red	Switch Departamento Técnico	Analista TI	Bajo	Mensual
Red	Switch Administrativo	Analista TI	Crítico	Diario
Red	Switch Comercial	Analista TI	Crítico	Diario
Red	Firewall Fortinet	Proveedor	Medio	Semanal
Red	Router	Proveedor	Bajo	Mensual
Red	Access Point Corporativo	Analista TI	Bajo	Mensual
Red	Access Point Comercial	Analista TI	Bajo	Mensual
Red	Access Point Técnico	Analista TI	Bajo	Mensual

7.5. TI-SEG-AN-03 Matriz de Criticidad para el Inventario de Activos

Una vez realizado el inventario de activos, es necesario clasificarlos de acuerdo con la importancia que tiene el activo dentro de la operación normal de la empresa.

Matriz Nivel de Criticidad de Activos					
Categoría	**Activo / Sistema**	**Descripción**	**Ubicación**	**Responsable**	**Criticidad**
Servidor	Vmware ESXI 7.0	Servidor Virtualizado 1	Rack TI	Analista TI	Crítico
Servidor	Vmware ESXI 7.1	Servidor Virtualizado 2	Rack TI	Analista TI	Crítico
Servidor	Windows Server 2019	Almacenamiento para Vcenter	Rack TI	Analista TI	Crítico
Servidor	NAS Synology	Almacenamiento	Rack TI	Analista TI	Alto
VoIP	UCM3626	Central de telefonía IP	Rack TI	Analista TI	Medio
VoIP	GrandStream	Teléfono IP x 15	Puesto Asignado	Analista TI	Bajo
Seguridad	NVR Hikvision	Central de cámaras de seguridad	Rack TI	Analista TI	Crítico
Seguridad	Cámara IP Hikvision	Cámara IP de seguridad x 16	Puesto Asignado	Analista TI	Alto
Seguridad	Reloj Biométrico ZKTeco	Control de asistencia	Puesto Control	Proveedor	Bajo
Aplicación	Microsoft 365	Correo y aplicaciones corporativas	Nube	Analista TI	Crítico
Aplicación	Kpax	Monitoreo de Impresoras	Nube	Analista TI	Bajo
Software	Vmware Vcenter	Gestión De Servidores Virtuales	Servidor Virtual	Analista TI	Crítico
Software	ESET	Antivirus	Servidor Virtual	Analista TI	Crítico
Software	PaperCut	Gestión de impresión	Servidor Virtual	Analista TI	Bajo
Software	Perseo	ERP	Servidor Virtual	Desarrollador TI	Crítico
Software	VeamBackup	Respaldos	Servidor Virtual	Analista TI	Crítico
Software	Directorio Activo	Registro de usuarios y equipos	Servidor Virtual	Analista TI	Crítico
Software	Directorio Activo 2	Respaldo de registro de usuarios y equipos	Servidor Virtual	Analista TI	Alto

Software	GLPI	Mesa de Ayuda Tecnología	Servidor Virtual	Analista TI	Bajo
Software	Service Desk	Mesa de Ayuda Clientes	Servidor Virtual	Analista TI	Medio
Software	Base de Datos	Base de datos de activos e historial de movimientos	Servidor Virtual	Desarrollador TI	Medio
Software	Sistema Activos	Movimientos de Inventario	Servidor Virtual	Desarrollador TI	Crítico
Software	OCS	Monitoreo de Activos Registrados	Servidor Virtual	Analista TI	Crítico
Red	Switch L3	Switch Core	Rack TI	Analista TI	Medio
Red	Switch L3	Switch Servidores	Rack TI	Analista TI	Bajo
Red	Switch L3	Switch Departamento Técnico	Rack TI	Analista TI	Bajo
Red	Switch L3	Switch Administrativo	Oficina Corporativas	Analista TI	Crítico
Red	Switch L3	Switch Comercial	Oficina Comercial	Analista TI	Crítico
Red	Firewall Fortinet	Seguridad perimetral	Rack TI	Proveedor	Medio
Red	Router	Router de Frontera	Rack TI	Proveedor	Bajo
Red	Access Point	WiFi corporativa	Oficina Corporativas	Analista TI	Bajo
Red	Access Point	WiFi Comercial	Oficina Comercial	Analista TI	Bajo
Red	Access Point	WiFi Departamento Técnico	Departamento Técnico	Analista TI	Bajo

8. Gestión de Incidentes y Continuidad

Se adopta un esquema de notificación y respuesta que incluye detección, contención, análisis, erradicación, recuperación y lecciones aprendidas. Para eventos que involucren datos personales, se aplican los plazos y obligaciones de notificación interna y registro que exige la normativa ecuatoriana, y la documentación de evidencias para auditoría BASC.

9. Evaluación de Desempeño, Auditoría y Mejora Continua

Se establecen indicadores de cobertura de inventario, tiempos de rotación de credenciales, tasas de cumplimiento de acceso por rol, incidentes de seguridad, y eficacia de restauración de backups. Se ejecutan auditorías internas periódicas conforme BASC V y revisiones por la dirección con acciones correctivas y de mejora.

10. Documentos Relacionados

TI-SEG-POL-04	Política de Seguridad Tecnológica
TI-GAT-POL-01	Política de Gestión de Activos Tecnológicos
TI-LAC-POL-01	Política de Licenciamiento y Actualización
TI-GAP-POL-01	Política de Gestión de Accesos y Privilegios
TI-INF-POL-02	Política de Clasificación de Información y Políticas de Acceso
TI-GSU-POL-01	Política de Gestión de Superusuarios y Continuidad de Credenciales
TI-BCP-POL-01	Política de Control de Dispositivos Externos
TI-SIM-POL-01	Política de Simulacros y Ejercicios
TI-INF-PL-02	Política de Clasificación de Información y Políticas de Acceso
TI-SEG-CRS-01	Criterios de seguridad para sistemas de TI
TI-GSU-PR-01	Procedimineto de Control de Superusuarios y Continuidad de Credenciales

TI-GSU-PR-01-A:	Procedimiento de Contingencia de Credenciales
TI-BCP-PR-01	Proceso de Respaldos y Restauración
TI-GAT-PR-01	Procedimiento de Baja y Eliminación Segura de Equipos
TI-BCP-PR-01	Procedimiento de Continuidad Operativa y Recuperación Ante Desastres
TI-INF-PR-02	Proceso de Clasificación de Información y Gestión de Accesos
TI-INF-AN-03	Inventario y Clasificación de la Información
TI-CRC-AN-03	Matriz de Criticidad de Cargos
TI-CRC-AN-04	Niveles de Criticidad Según cada Cargo
TI-BCK-AN-03	Matriz de Frecuencia y Criticidad de Respaldo
TI-SEG-AN-03	Matriz de Criticidad para el Inventario de Activos

C.Anexo: TI-SEG-POL-04

POLÍTICA DE SEGURIDAD TECNOLÓGICA DE LA EMPRESA DE SERVICIOS ELECTRÓNICOS

Código: TI-SEG-POL-04
Versión: 1.0
Fecha: _____
Aprobado por: Gerencia General

1. Objetivo

El propósito de esta Política de Seguridad Tecnológica es establecer las directrices que orientan la protección, gestión y recuperación de los sistemas de tecnologías de la información de la organización, garantizando que todos los recursos tecnológicos sean gestionados de manera segura, responsable y coherente con los objetivos del negocio. Esta política se desarrolla en cumplimiento del control 6.2.a del estándar BASC y se fundamenta en los lineamientos establecidos por la norma ISO/IEC 27001:2022 para la gestión de la seguridad de la información.

2. Alcance

La política aplica a todos los sistemas, servicios tecnológicos, infraestructura de red, servidores físicos y virtuales, aplicaciones locales o en la nube, bases de datos, equipos informáticos y dispositivos móviles utilizados por la organización. Su cumplimiento es obligatorio para todo el personal interno, así como para colaboradores externos que, por la naturaleza de sus funciones, accedan a la infraestructura tecnológica o a la información institucional.

3. Marco Normativo

La implementación de esta política se basa en los requerimientos establecidos por el estándar BASC y en las disposiciones de ISO 27001:2022, considerando los controles relacionados con la seguridad organizacional, la gestión de activos, la gestión de accesos, la protección de sistemas, la operación segura, el desarrollo y mantenimiento tecnológico, así como la continuidad del negocio. Adicionalmente, incorpora las obligaciones legales y regulatorias aplicables a la protección de datos, al manejo de información sensible y a la operación tecnológica.

4. Principios de Seguridad Tecnológica

La gestión de la seguridad tecnológica se orienta bajo cuatro principios fundamentales: la confidencialidad, entendida como la obligación de garantizar que la información esté disponible únicamente para quienes tienen autorización; la integridad, relacionada con la protección de la exactitud y completitud de los datos; la disponibilidad, que implica asegurar que los sistemas y servicios puedan ser utilizados cuando el negocio lo requiera; y la capacidad de recuperación, que exige mantener mecanismos que permitan restaurar los sistemas después de interrupciones, incidentes o fallas.

5. Lineamientos Generales para la Gestión Tecnológica

Los lineamientos a continuación expuestos son de

5.1. Gestión de Activos Tecnológicos

- Todo sistema y servicio tecnológico debe estar debidamente registrado en un inventario actualizado que permita su identificación, seguimiento y control. Este registro constituye la base para la gestión de activos y garantiza la trazabilidad de cada componente dentro de la infraestructura tecnológica.
- Cada activo tecnológico debe contar con un propietario claramente asignado, responsable de su administración, mantenimiento y cumplimiento de las políticas de seguridad. Esta asignación asegura la rendición de cuentas y facilita la toma de decisiones en caso de incidentes o cambios operativos.
- La matriz de criticidad debe actualizarse de manera periódica, preferiblemente de forma anual o cuando se produzcan cambios significativos en la infraestructura, procesos o riesgos asociados. Esta práctica permite mantener vigente la clasificación de activos y asegurar que las medidas de protección se ajusten a la realidad de la empresa.

5.2. Protección de Sistemas

- Los sistemas deben disponer de controles de protección proporcionales a su nivel de criticidad, garantizando que los activos más sensibles cuenten con mecanismos robustos para prevenir accesos no autorizados, pérdida de datos o interrupciones en el servicio.
- Es indispensable implementar mecanismos de seguridad como soluciones antivirus, aplicación de parches de seguridad, firewalls, cifrado de información y herramientas de monitoreo continuo. Estas medidas reducen la superficie de ataque y fortalecen la resiliencia frente a amenazas internas y externas.
- Los servicios considerados críticos deben estar segmentados dentro de la red y reforzados mediante técnicas de endurecimiento (*hardening*), eliminando configuraciones inseguras y limitando vectores de ataque.

5.3. Control de Accesos

- Todo acceso a sistemas y aplicaciones debe regirse por el principio de mínimos privilegios, otorgando únicamente los permisos estrictamente necesarios para el desempeño de las funciones asignadas.
- Las credenciales de acceso de los usuarios a los sistemas de la empresa son únicas e individuales, y cualquier usuario que las transfiera a otro usuario o usuarios, se considerará como una falta grave. Las contraseñas de acceso de los usuarios deben cumplir con los parámetros mínimos, listados a continuación, para cumplir con el estándar de seguridad:
    - Longitud: 12 caracteres
    - Complejidad: 1 mayúscula, 1 minúscula, 1 símbolo y 1 alfanumérico.
    - Historial: No repetir las últimas dos contraseñas anteriores (si lo permite)
    - Caducidad: renovación cada 90 días.

- En los sistemas críticos se debe aplicar autenticación multifactor, incorporando mecanismos adicionales de verificación para reducir el riesgo de accesos indebidos.
- Las cuentas de usuario deben ser revisadas de manera periódica y deshabilitadas inmediatamente al finalizar la relación laboral o contractual, evitando que credenciales inactivas se conviertan en un punto de vulnerabilidad.

5.4. Continuidad del Negocio

- Los sistemas críticos deben tener definidos y documentados sus parámetros de RTO (Recovery Time Objective) y RPO (Recovery Point Objective), asegurando que los objetivos de recuperación estén alineados con la estrategia de continuidad del negocio.
- La organización debe contar con un Plan de Recuperación ante Desastres (DRP) formalmente establecido y realizar pruebas periódicas para validar su efectividad y garantizar la capacidad de respuesta ante incidentes mayores.
- Las copias de seguridad deben ejecutarse y verificarse de manera regular, asegurando la integridad de los datos y la disponibilidad de la información en caso de contingencias.

5.5. Gestión de Cambios Tecnológicos

- Todo cambio en la infraestructura tecnológica debe ser planificado y registrado, siguiendo un proceso controlado que minimice riesgos y garantice la trazabilidad de las modificaciones.
- Los sistemas críticos requieren autorización previa de Gerencia General antes de aplicar cualquier cambio significativo, asegurando que las decisiones se tomen bajo criterios técnicos y de seguridad.
- Se deben mantener versiones anteriores y procedimientos de reversión (rollback) para garantizar la recuperación ante fallos durante la implementación de cambios).

5.6. Monitoreo y Auditoría

- Los sistemas críticos deben generar y conservar registros de auditoría que permitan monitorear actividades, detectar anomalías y cumplir con los requisitos normativos.
- El área de TI debe realizar revisiones periódicas de los registros de eventos, alertas y actividades sospechosas, aplicando análisis proactivo para prevenir incidentes.
- Cualquier anomalía detectada debe ser gestionada conforme al proceso formal de tratamiento de incidentes, asegurando una respuesta rápida, documentada y alineada con las políticas de seguridad.

6. Responsabilidades

Gerencia General

- Aprobar la política y garantizar su cumplimiento.

Analista de TI

- Implementar los criterios de seguridad.
- Mantener actualizada la documentación técnica.
- Supervisar la correcta ejecución de respaldos, parches y controles.

Responsables de los Sistemas

- Asegurar que sus sistemas cumplan con los controles establecidos.
- Aprobar accesos y validar la criticidad asignada.

Usuarios

- Usar los sistemas de forma adecuada y cumplir con todas las medidas de seguridad aplicables.

7. Documentación Necesaria para el Cumplimiento

La organización deberá mantener actualizados el inventario de activos tecnológicos y la matriz de criticidad de sistemas y servicios. Asimismo, se requiere contar con criterios de seguridad por nivel de criticidad, procedimientos de respaldo y restauración, un plan de continuidad operativa, un plan de recuperación ante desastres, procedimientos de gestión de accesos y de gestión de cambios, además de políticas complementarias sobre uso aceptable y protección de la información. La evidencia de respaldos, restauraciones, auditorías, incidentes y mantenimiento deberá conservarse como parte del soporte documental para auditorías internas y externas.

8. Revisión y Actualización

La política será revisada anualmente, o antes si se producen cambios significativos en la infraestructura tecnológica, en el modelo operativo o en los requerimientos regulatorios. Cualquier modificación deberá ser aprobada por la Gerencia General antes de entrar en vigencia.

Versión	Fecha	Descripción	Responsable
1.0	_____	Emisión inicial	_____

D. Anexo: TI-SEG-CRS-01

CRITERIOS DE SEGURIDAD PARA SISTEMAS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA EMPRESA DE SERVICIOS ELECTRÓNICOS

Código: TI-SEG-CRS-01
Versión: 1.0
Fecha: _____
Aprobado por: _____

1. Objetivo

Establecer, documentar y mantener criterios de seguridad que permitan identificar, proteger y garantizar la recuperación oportuna de los sistemas de tecnologías de la información de la organización, en conformidad con el control **6.2.a del estándar BASC** y los requisitos de **ISO 27001:2022 (Controles A.5, A.8, A.9, A.12, A.14 y A.17)**.

2. Alcance

Este documento aplica a todos los sistemas de información, aplicaciones, servidores, bases de datos, servicios en la nube, infraestructura de red y cualquier componente tecnológico identificado en el **inventario de activos** y categorizado en la **matriz de criticidad de sistemas y servicios** vigente.

3. Responsabilidades

- **Responsable de TI:** asegurar la implementación y actualización de los criterios.
- **Propietarios de activos:** validar los criterios de seguridad asociados a sus sistemas.
- **Usuarios:** cumplir con los controles definidos.
- **Equipo de Seguridad/Comité:** revisar y aprobar cambios basados en riesgos.

4. Base para la Aplicación de los Criterios

Los criterios de seguridad se asignan según la **criticidad del sistema**, determinada por:

- Confidencialidad
- Integridad
- Disponibilidad
- Impacto en el negocio
- Dependencias operativas
- Obligaciones legales, regulatorias y contractuales

Las categorías aplicadas son:

- Alta criticidad
- Media criticidad
- Baja criticidad

5. Criterios de Seguridad por Nivel de Criticidad

5.1 Controles Generales Obligatorios para Todos los Sistemas

Estos controles aplican independientemente de la criticidad:

5.1.1 Protección Básica

- Antivirus/EDR habilitado y actualizado.
- Políticas de contraseñas según ISO/A.8.2.3.

- Parcheo mínimo mensual.
- Copias de seguridad según política vigente.
- Registro y gestión de incidentes.
- Respaldo documentado del sistema en el inventario.

5.1.2 Gestión de Accesos

- Accesos basados en roles.
- Revisión semestral de permisos otorgados.
- Deshabilitación inmediata de cuentas inactivas.

5.1.3 Cumplimiento Normativo

- Aplicación de restricciones sobre datos personales según legislación local.
- Revisión anual de requisitos legales y contractuales específicos.

5.2 Criterios para Sistemas de Alta Criticidad (Críticos)

Aplica a sistemas cuya interrupción detiene la operación o genera pérdidas significativas.

5.2.1 Protección Avanzada

- Autenticación multifactor obligatoria.
- Cifrado de datos en tránsito y en reposo.
- Segmentación de red y aislamiento.
- Endurecimiento (hardening) obligatorio.
- Monitoreo continuo y alertas automáticas.

5.2.2 Continuidad y Recuperación

- RTO ≤ 4 horas / RPO ≤ 1 hora.
- Pruebas de recuperación semestrales.
- Backups diarios y almacenamiento fuera del sitio.

5.2.3 Auditoría y Trazabilidad

- Log de auditoría obligatorio, con retención mínima de 12 meses.
- Revisión de logs por el área de TI al menos una vez al mes.

5.2.4 Gestión de Cambios

- Cambios bajo aprobación del Comité de TI.
- Control estricto de versiones y rollback documentado.

5.3 Criterios para Sistemas de Media Criticidad

Aplica a servicios importantes pero que no detienen por completo la operación.

5.3.1 Protección Media

- Parches aplicados dentro de 15 días.
- Cifrado en tránsito obligatorio.
- MFA recomendado, obligatorio para administradores.
- Hardening básico.

5.3.2 Continuidad

- RTO ≤ 24 horas / RPO ≤ 8 horas.
- Copias de seguridad cada 48–72 horas.

5.3.3 Trazabilidad

- Activación de logs básicos.
- Revisión trimestral.

5.4 Criterios para Sistemas de Baja Criticidad

Aplica a sistemas complementarios o de apoyo.

5.4.1 Protección mínima requerida

- Antivirus activo.
- Parcheo trimestral.
- Acceso basado en roles.

5.4.2 Continuidad

- RTO ≤ 72 horas / RPO ≤ 24 horas.
- Backups semanales o según necesidad.

6. Criterios Específicos por Tipo de Activo

6.1 Servidores Físicos o Virtuales

- Inventariados con especificación técnica.
- Restricción de puertos y servicios innecesarios.
- Monitoreo de CPU, red, disco y servicios.

6.2 Aplicaciones y Software

- Validaciones de integridad del código.
- Control de versiones.
- Pruebas de seguridad antes de cambios mayores.

6.3 Bases de Datos

- Cifrado obligatorio (medios críticos o altos).
- Acceso restringido por roles.
- Monitoreo de consultas inusuales.

6.4 Equipos de Red

- Uso obligatorio de contraseñas robustas y MFA cuando aplique.
- Configuración segura respaldada.
- Segmentación de VLAN para sistemas críticos.

6.5 Servicios Cloud

- Evaluación del proveedor (SLA, certificaciones).
- Garantía de ubicación y control de datos.
- Cifrado y MFA obligatorio.

7. Mantenimiento de los Criterios

- Revisión anual o posterior a incidentes.
- Validación contra cambios tecnológicos o regulatorios.
- Actualización basada en evaluación de riesgos.

8. Evidencias Requeridas

- Inventario vigente

- Matriz de criticidad actualizada
- Informes de backup y restauración
- Logs de auditoría
- Registros de incidentes
- Informes de pruebas DRP
- Bitácoras de mantenimiento
- Aprobaciones de cambio

Versión	Fecha	Descripción del Cambio	Responsable
1.0	_____	Creación del documento	_____

E. Anexo: TI-GAT-POL-01

POLÍTICA DE GESTIÓN DE ACTIVOS TECNOLÓGICOS DE LA EMPRESA DE SERVICIOS ELECTRÓNICOS

Código: TI-GAT-POL-01
Versión: 1.0
Aprobado por: Gerencia General
Fecha: ___ / ___ / _____

1. Objetivo

Establecer los lineamientos generales para la identificación, administración, uso, protección y control de los activos tecnológicos de la organización, garantizando su integridad, disponibilidad y confidencialidad, en cumplimiento del Sistema de Gestión en Control y Seguridad BASC.

2. Alcance

Aplica a todos los activos tecnológicos propiedad de la empresa o bajo su responsabilidad, incluyendo hardware, software, información digital, servicios tecnológicos, redes, cuentas de usuario y cualquier recurso utilizado para el procesamiento de información.

3. Principios de la Política

a) **Identificación y Registro:** Todo activo tecnológico debe estar registrado en el Inventario Oficial de Activos.
b) **Asignación de Responsables:** Cada activo tendrá un custodio designado responsable de su uso y protección.
c) **Clasificación por Criticidad:** Los activos serán clasificados según su importancia operativa y riesgo asociado.
d) **Uso Aceptable:** Los activos se utilizarán únicamente para fines autorizados por la organización.
e) **Protección y Seguridad:** Se implementarán controles para garantizar la confidencialidad, integridad y disponibilidad de la información.
f) **Ciclo de Vida:** Los activos serán gestionados desde su adquisición hasta su baja definitiva.
g) **Revisión:** La política será revisada anualmente o cuando existan cambios significativos en los activos o en el SGCS BASC.

4. Responsabilidades

Gerencia General
Aprobar la política y asignar recursos financieros, tecnológicos y humanos requeridos para su el cumplimiento.
Área de TI
Administrar el inventario, aplicar controles, ejecutar procedimientos asociados.
Usuarios y Custodios
Utilizar y proteger adecuadamente los activos asignados.
Representantes del SGCS BASC
Verificar cumplimiento y reportar observaciones.

5. Cumplimiento

Las acciones correctivas derivadas serán gestionadas de acuerdo con los procedimientos internos del sistema de gestión, asegurando su seguimiento hasta su implementación total. Esta política es de cumplimiento obligatorio para todas las áreas involucradas y constituye un elemento esencial para fortalecer la seguridad tecnológica y la continuidad operativa de la organización.

Versión	Fecha	Descripción	Responsable
1.0	_____	Emisión inicial	_____

F. Anexo: TI-GAT-PR-01

PROCEDIMIENTO DE BAJA Y ELIMINACIÓN SEGURA DE EQUIPOS INFORMÁTICOS DE LA EMPRESA DE SERVICIOS ELECTRÓNICOS

Código: TI-GAT-PR-01
Versión: 1.0
Aprobado por: Gerencia General
Fecha: ___ / ___ / _____

1. Objetivo

Establecer los pasos y controles necesarios para la desincorporación, baja y eliminación segura de equipos informáticos, asegurando la protección de la información y el cumplimiento de normativas BASC.

2. Alcance

Aplica a equipos informáticos, periféricos y dispositivos de almacenamiento propiedad de la organización.

3. Definiciones

- **Baja:** Proceso mediante el cual un equipo se retira permanentemente del inventario activo.
- **Eliminación Segura:** Proceso de borrado, destrucción o sobreescritura de información que garantiza que no podrá ser recuperada.
- **Acta de Baja:** Documento formal que certifica la desincorporación de un activo.

4. Procedimiento

4.1 Solicitud de Baja

- El custodio o supervisor reporta la necesidad de baja a TI mediante formulario o ticket.
- TI evalúa el estado del equipo: obsoleto, dañado, pérdida de soporte o reemplazo.

4.2 Aprobación

- TI remite informe de verificación.
- Gerencia o Jefatura autorizan la baja mediante firma o aprobación digital.

4.3 Respaldo de Información

- TI valida que el usuario haya respaldado toda la información necesaria.
- Se elimina cualquier cuenta o acceso vinculado.

4.4 Eliminación Segura de Datos

TI deberá aplicar uno de los siguientes métodos:

- Sobreescritura segura (wipe) de discos.
- Formateo seguro con algoritmos aprobados.
- Destrucción física del medio (si el equipo no enciende o el disco está dañado).

- Certificado de destrucción, si se usa un proveedor externo.

Todo proceso debe quedar documentado en el **Registro de Baja**.

4.5 Retiro del Inventario

- TI actualiza el Inventario de Activos.
- Se registra el estado final del equipo (chatarra, donación, reciclaje, destruido).

4.6 Disposición Final

Opciones autorizadas:

- Entrega a gestor ambiental certificado.
- Destrucción del hardware en la empresa con evidencia fotográfica.
- Donación aprobada por Gerencia (sin discos duros operativos).

4.7 Acta de Baja

Incluye:

- Código del activo
- Descripción
- Responsable
- Motivo de baja
- Método de eliminación segura
- Autorizaciones
- Evidencias adjuntas

5. Responsabilidades

- **TI:** Ejecutar el procedimiento y documentar evidencias.
- **Gerencia:** Autorizar bajas y donaciones.
- **Usuarios:** Entregar equipos en estado y respaldar información.

Versión	Fecha	Descripción	Responsable
1.0	_____	Emisión inicial	_____

G.Anexo: TI-GAT-RG-01

REGISTRO DE INVENTARIOS PERIÓDICOS DE ACTIVOS TECNOLÓGICOS PARA LE EMPRESA DE SERVICIOS ELECTRÓNICOS

Código: TI-GAT-RG-01
Versión: 1.0
Uso: Registro interno
Fecha: ___ / ___ / _____

1. Objetivo del Registro

Documentar los resultados de las verificaciones periódicas del Inventario de Activos Tecnológicos para garantizar su existencia, ubicación, estado y responsabilidad, conforme a los controles BASC.

2. Frecuencia de Aplicación

- Mínimo **1 vez al año** o según determine el SGCS BASC.
- Puede realizarse por área, por tipo de activo o de forma total.

3. Campos del Registro

Activo	Descripción	Serie	Ubicación	Custodio	Validación	Observación	Responsable	

4. Almacenamiento del Registro

- Debe ser archivado por TI por un periodo no menor a 3 años.
- Puede almacenarse en formato digital o físico.
- Sirve como evidencia de auditoría BASC.

Versión	Fecha	Descripción	Responsable
1.0	_____	Emisión inicial	_____

H. Anexo: TI-BCP-POL-01

POLÍTICA DE CONTROL DE DISPOSITIVOS EXTERNOS Y PERIFÉRICOS NO AUTORIZADOS DE LA EMPRESA DE SERVICIOS ELECTRÓNICOS

Código: TI-BCP-POL-01
Versión: 1.0
Aprobado por: Gerencia General
Fecha: ___ / ___ / _____

1. Objetivo

Establecer los lineamientos para restringir, controlar y autorizar la conexión de dispositivos externos, dispositivos personales (BYOD) y periféricos no autorizados a cualquier equipo que forme parte de la infraestructura informática de la organización, con el fin de prevenir riesgos de seguridad, fuga de información o introducción de software malicioso.

2. Alcance

Esta política aplica a todos los usuarios internos, personal externo, contratistas y visitantes que tengan acceso a recursos tecnológicos de la empresa, así como a todos los equipos informáticos, periféricos y dispositivos de almacenamiento que pertenezcan a la infraestructura tecnológica institucional. Queda estrictamente prohibida la conexión de dispositivos personales, tales como memorias USB, discos duros externos, teléfonos móviles utilizados para transferencia de datos y cualquier periférico que no haya sido previamente autorizado por el área de Tecnologías de la Información.

3. Principios de la Política

3.1 Prohibición de Dispositivos Personales

Queda estrictamente prohibida la conexión de dispositivos personales tales como:

- Memorias USB
- Discos duros externos
- Teléfonos móviles para transferencia de archivos
- Periféricos no corporativos (teclados, mouse, adaptadores, cámaras, etc.)

3.2 Uso de Periféricos Autorizados

Solo se permite el uso de dispositivos y periféricos inventariados, codificados y aprobados por el área de TI. Cualquier equipo no registrado se considerará **no autorizado**.

3.3 Controles Técnicos Obligatorios

El área de TI deberá implementar controles que garanticen la aplicación de esta política, tales como:

- Restricción de puertos USB
- Software de control de dispositivos (Device Control)
- Políticas de grupo (GPO)
- Monitoreo de intentos de conexión

3.4 Excepciones Controladas

Cualquier excepción deberá:

- Ser solicitada por escrito
- Ser aprobada por TI y/o Gerencia

- Contar con un justificativo técnico-operativo
- Ser registrada como evidencia BASC

3.5 Protección de la Información

No se permitirá la copia, extracción o transferencia de información a dispositivos externos no corporativos en ninguna circunstancia.

4. Responsabilidades

Gerencia General

La Gerencia General es responsable de aprobar esta política y garantizar que se destinen los recursos necesarios para su aplicación.

Área de TI

El área de TI es responsable de administrar los periféricos autorizados, mantener los controles técnicos de restricción y supervisar el cumplimiento de las disposiciones aquí establecidas.

Usuarios y Personal Interno

Todos los usuarios deben acatar esta política y reportar cualquier intento de conexión no autorizada o situaciones que puedan representar un riesgo para la seguridad de los sistemas.

Representante BASC

Verificará periódicamente el cumplimiento de esta política y documentará las observaciones o desviaciones encontradas.

5. Sanciones por Incumplimiento

El incumplimiento de estas disposiciones podrá dar lugar a las acciones correctivas o disciplinarias definidas por la empresa, sin perjuicio de la aplicación de análisis de incidentes o medidas adicionales cuando se detecten riesgos significativos para la seguridad. Esta política será revisada de manera anual, o antes si existieran cambios relevantes en la infraestructura tecnológica, en los requisitos BASC o en los riesgos asociados al uso de dispositivos externos.

6. Revisión y Actualización

Esta política será revisada de manera anual, o antes si existieran cambios relevantes en la infraestructura tecnológica, en los requisitos BASC o en los riesgos asociados al uso de dispositivos externos.

Versión	Fecha	Descripción	Responsable
1.0	_____	Emisión inicial	_____

I. Anexo: TI-BCP-PR-01

PROCEDIMIENTO DE RESPALDOS Y RESTAURACIÓN DE LA EMPRESA DE SERVICIOS ELECTRONICOS

Código: TI-BCP-PR-01
Versión: 1.0
Fecha: _____
Aprobado por: Gerencia General

1. Objetivo

El propósito de este procedimiento es establecer las directrices y actividades necesarias para asegurar la protección, disponibilidad, integridad y recuperación oportuna de la información y los sistemas utilizados por la organización, mediante la ejecución controlada de respaldos y procesos de restauración.

2. Alcance

Este procedimiento aplica a toda la información y sistemas incluidos en el **Inventario de Activos**, particularmente aquellos clasificados como críticos en la **Matriz de Criticidad de Activos**, y comprende tanto los respaldos locales y externos como su adecuada restauración ante incidentes, fallas, alteraciones, ataques o eventos que amenacen la continuidad operativa.

3. Fundamentación BASC y relación con el SGCS

Este procedimiento se integra al SGCS BASC como control preventivo y de recuperación. Contribuye al cumplimiento de:

- **Capítulo 6 – Seguridad de la Información**, apartado 6.2 a.
- Controles de continuidad operativa establecidos en el SGCS.
- Controles asociados a manejo seguro de información sensible dentro de procesos de la cadena de suministro.

La correcta ejecución y actualización de este procedimiento es un requisito para asegurar la trazabilidad, confiabilidad y resiliencia de los sistemas de TI.

4. Responsabilidades

El área de Tecnología de la Información es la responsable de gestionar la programación, ejecución, monitoreo y custodia de los respaldos, así como de realizar las restauraciones cuando sean requeridas.
Los propietarios de la información deben notificar cualquier cambio en sistemas, bases de datos o estructuras que afecten la estrategia de respaldo definida. El Comité BASC supervisa el cumplimiento y la integridad de los registros.

5. Lineamientos generales del procedimiento

5.1. Estrategia de respaldo

Los respaldos se ejecutan conforme a la criticidad definida por la organización:

- Los activos **críticos** se respaldan diariamente, combinando un respaldo completo semanal con respaldos incrementales o diferenciales diarios.
- Los activos **moderados** se respaldan con una frecuencia no mayor a 72 horas.

- Los activos de **baja criticidad** se respaldan semanalmente o según necesidades del proceso.
- La estrategia se documenta en la **Matriz de Respaldo del SGCS**.

5.2. Almacenamiento y protección

Todos los respaldos se almacenan en ubicaciones seguras, utilizando al menos dos medios independientes: repositorio interno y repositorio externo (nube o sitio alterno).
Los respaldos deben implementarse con cifrado y acceso restringido, conforme a los controles de seguridad definidos por BASC.

5.3. Ejecución del respaldo

La ejecución se realiza de forma automatizada o manual según el sistema, generando registros verificables. Las tareas de respaldo deben contar con monitoreo continuo y alertas que permitan identificar fallas o inconsistencias.

5.4. Pruebas de restauración

Periódicamente, y como requisito del SGCS, se realizan pruebas de restauración para verificar la integridad de los respaldos y la capacidad de recuperación dentro de los tiempos establecidos. Los resultados se registran y se presentan en la Revisión por la Dirección cuando corresponda.

6. Procedimiento de Restauración

La restauración se activa ante incidentes, fallas operativas o solicitud del propietario del proceso.
TI selecciona el respaldo más adecuado según su fecha, integridad y disponibilidad, ejecuta el proceso en los ambientes autorizados y documenta los resultados.
El usuario valida la información restaurada, asegurando que cumple con la integridad necesaria para la continuidad del proceso operativo.

7. Seguridad de los respaldos

El acceso a los respaldos se encuentra restringido al personal autorizado. Los medios físicos deben permanecer asegurados en espacios controlados, y los respaldos digitales deben almacenarse bajo cifrado y en repositorios con autenticación reforzada. Todos los accesos y manipulaciones quedan registrados como evidencia del SGCS.

8. Registros generados

Este procedimiento genera los siguientes registros obligatorios para auditoría BASC:

- Registro de trabajo de respaldos (logs del sistema).
- Registro de fallas en respaldos.
- Registro de restauraciones realizadas.
- Reportes de pruebas de restauración.
- Matriz de Frecuencia y Criticidad de Respaldo.

Se deben conservar conforme al procedimiento de control documental del SGCS.

9. Revisión y Mejora Continua

El presente procedimiento se revisa al menos una vez al año o cuando existan cambios significativos en la infraestructura tecnológica, riesgos identificados, requisitos legales o

actualizaciones del estándar BASC. Su eficacia se evalúa mediante auditorías internas y análisis de incidentes.

Versión	Fecha	Descripción	Responsable
1.0	_____	Emisión inicial	_____

J. Anexo: TI-BCP-PR-02

PROCEDIMIENTO DE CONTINUIDAD OPERATIVA Y RECUPERACIÓN ANTE DESASTRES DE LA EMPRESA DE SERVICIOS ELECTRÓNICOS

Código: TI-BCP-PR-02
Versión: 1.0
Fecha: _____
Aprobado por: Gerencia General

1. Objetivo

El objetivo de este procedimiento es establecer las actividades necesarias para asegurar la continuidad de los servicios tecnológicos y la recuperación oportuna de los sistemas de información en caso de interrupciones, incidentes mayores, desastres u otros eventos que comprometan la operación. Este procedimiento se desarrolla en cumplimiento del control 6.2.a del estándar BASC y de los requisitos del control A.17 de ISO 27001:2022 relacionados con la continuidad del negocio y la resiliencia tecnológica.

2. Alcance

El presente procedimiento aplica a todos los sistemas críticos y esenciales identificados en la matriz de criticidad de la organización, incluyendo servidores, bases de datos, aplicaciones, servicios en la nube, infraestructura de red y cualquier componente tecnológico cuyo funcionamiento sea indispensable para la operación continua del negocio. También comprende las actividades del personal responsable de TI, propietarios de sistemas y usuarios clave durante situaciones de contingencia.

3. Definiciones

Para fines de este documento, se entiende como continuidad operativa la capacidad de mantener o restablecer las actividades esenciales del negocio ante eventos disruptivos. La recuperación ante desastres se refiere al conjunto de acciones que permite restaurar sistemas tecnológicos, servicios y datos después de fallas críticas, incidentes de ciberseguridad, daños físicos o desastres naturales. Los términos RTO (Recovery Time Objective) y RPO (Recovery Point Objective) se utilizan para establecer los tiempos máximos permitidos de recuperación y pérdida de datos, respectivamente, según la criticidad de cada sistema.

4. Responsabilidades

La Gerencia General

Es responsable de aprobar el plan y asegurar la disponibilidad de los recursos necesarios para su ejecución.

Analista TI

es responsable de liderar las actividades de respuesta, evaluar el impacto, activar los planes de contingencia y coordinar la recuperación de los sistemas afectados.

Responsables de sistemas

Deben validar los tiempos de recuperación establecidos y colaborar en la priorización de actividades.

Usuarios

Deberán ejecutar las tareas asignadas para la continuidad de procesos y validar la correcta restauración de los servicios.

5. Activación del Plan

El procedimiento se activa cuando ocurre un evento que afecte la operación normal de los sistemas de TI. El Analista TI determinará, con base en la matriz de criticidad y el impacto del incidente, si se requiere activar la fase de contingencia o el plan completo de recuperación. Una vez confirmada la interrupción, el responsable notificará a la Gerencia General y a los Responsables de los sistemas afectados, documentará la naturaleza del incidente y definirá las acciones inmediatas para contener o mitigar el daño.

6. Contención Inicial

Durante la fase de contención se evalúa la magnitud del incidente, se identifica la causa probable y se define la estrategia temporal para mantener la operación mínima indispensable.

Esto puede incluir el uso de sistemas alternos, el aislamiento de segmentos de red, la desactivación temporal de servicios afectados o el uso de respaldos operativos.

Todas las acciones deben registrarse en la bitácora de incidentes para garantizar trazabilidad.

7. Procedimiento de Continuidad (BCP)

La continuidad operativa consiste en mantener la funcionalidad mínima de los procesos críticos. Una vez activado el procedimiento de continuidad, los responsables ejecutarán las actividades previamente definidas para garantizar que las áreas del negocio puedan seguir operando.

Esto incluye el uso de documentación impresa o respaldos locales, el traslado a ubicaciones alternas cuando corresponda, la utilización de sistemas secundarios o el empleo de mecanismos temporales de comunicación.

El Analista TI deberá verificar que los procesos esenciales se mantengan dentro de los parámetros de tiempo establecidos y garantizar que los usuarios clave tengan acceso a los recursos mínimos necesarios.

8. Procedimiento de Recuperación ante Desastres (DRP)

Cuando la interrupción exceda las capacidades de continuidad operativa, se inicia formalmente la fase de recuperación ante desastres.

Durante esta fase, TI procederá a restaurar los servicios siguiendo el orden de prioridad definido en la matriz de criticidad.

Los sistemas más críticos se restaurarán primero, respetando los valores de RTO y RPO previamente definidos.

La restauración deberá realizarse desde respaldos validados, repositorios alternos o infraestructura secundaria según corresponda.

Posteriormente, se realizará la verificación de integridad de datos, pruebas funcionales y certificación por parte de los propietarios de sistemas antes de restablecer los servicios al ambiente productivo.

9. Validación y Retorno a la Operación Normal

Una vez que los sistemas hayan sido restaurados y verificados, los propietarios de los activos confirmarán formalmente que la funcionalidad es correcta y que los datos recuperados cumplen con los parámetros establecidos. Solo después de esta validación se realizará el retorno a la operación normal. El Analista TI informará oficialmente a la Gerencia General sobre la recuperación exitosa, documentará los tiempos de restablecimiento y elaborará un informe post-incidente detallando causas, acciones ejecutadas y recomendaciones de mejora.

10. Pruebas del Plan

El plan de continuidad y recuperación será probado como mínimo una vez al año, o inmediatamente después de actualizaciones significativas en la infraestructura tecnológica, cambios en procesos esenciales o incidentes graves. Las pruebas pueden incluir simulaciones, restauraciones parciales, ejercicios de escritorio y conmutación hacia ambientes alternos. Los resultados se documentarán y se emplearán para actualizar el procedimiento y fortalecer la capacidad de respuesta de la organización.

11. Revisión y Actualización

El presente procedimiento será revisado de forma anual o cada vez que se produzcan cambios relevantes en los servicios críticos, la infraestructura tecnológica o las funciones operativas. Las actualizaciones deberán ser aprobadas por la Dirección General y comunicadas a todo el personal involucrado.

Versión	Fecha	Descripción	Responsable
1.0	_____	Emisión inicial	_____

K. Anexo: TI-INF-POL-02

POLITICA DE CLASIFICACIÓN DE INFORMACIÓN Y POLÍTICAS DE ACCESO DE LA EMPRESA DE SERVICIOS ELECTRÓNICOS

Código sugerido: TI-INF-POL-02
Versión: 1.0
Aprobado por: Gerencia General
Fecha: ___ / ___ / _____

1. Objetivo

Establecer lineamientos para la clasificación de la información conforme a la legislación vigente en Ecuador (LOPDP) y la norma BASC V, definiendo políticas de acceso basadas en niveles de criticidad.

2. Alcance

Aplica a toda la información generada, procesada y almacenada por la organización, incluyendo datos personales, operativos y estratégicos

3. Principios de la Política

La organización clasificará la información en niveles de criticidad y establecerá políticas de acceso basadas en roles y necesidad operativa. Se aplicarán controles técnicos y organizativos para garantizar la confidencialidad, integridad y disponibilidad, cumpliendo con la LOPDP y BASC V.

Nivel	Descripción
Crítico	Datos personales, credenciales, información financiera, datos BASC
Confidencial	Información operativa interna, procesos logísticos
Público	Información divulgable sin riesgo

4. Responsabilidades

Gerencia General
Aprobar la política y asignar recursos financieros, tecnológicos y humanos requeridos para su el cumplimiento
Área de TI
Administración de cuentas, implementación técnica, monitoreo y mantenimiento de controles.
Representantes del SGCS BASC
Aprobación de excepciones, verificación de cumplimiento y reportar observaciones.
Encargado de Procesos
Control documental y auditoría interna.

5. Cumplimiento

Las acciones correctivas derivadas serán gestionadas de acuerdo con los procedimientos internos del sistema de gestión, asegurando su seguimiento hasta su implementación total. Esta política es de cumplimiento obligatorio para todas las áreas

involucradas y constituye un elemento esencial para fortalecer la seguridad tecnológica y la continuidad operativa de la organización.

Versión	Fecha	Descripción	Responsable
1.0	_____	Emisión inicial	_____

L. Anexo: TI-GAP-POL-01

POLÍTICA DE GESTIÓN DE ACCESOS Y PRIVILEGIOS DE LA EMPRESA DE SERVICIOS ELECTRÓNICOS

Código: TI-GAP-POL-01
Versión: 1.0
Fecha de Emisión: ___ / ___ / ____
Aprobación: Gerencia General

1. Objetivo

Establecer los lineamientos para la asignación, control y revisión de accesos y privilegios a sistemas, aplicaciones y recursos tecnológicos, garantizando que dichos accesos se otorguen conforme al principio de mínimos privilegios y en función de las responsabilidades asignadas, en cumplimiento con el estándar BASC y las mejores prácticas internacionales.

2. Alcance

Esta política aplica a todos los colaboradores, contratistas y terceros que requieran acceso a sistemas, aplicaciones, bases de datos, redes y cualquier recurso tecnológico de la organización.

3. Principios

- **Mínimos privilegios:** Cada usuario dispondrá únicamente de los permisos necesarios para el desempeño de sus funciones.
- **Segregación de funciones:** Se evitará la acumulación de privilegios que pueda generar conflictos de interés o riesgos operativos.
- **Revisión periódica:** Los accesos serán revisados de forma regular para garantizar su vigencia y pertinencia.
- **Autenticación reforzada:** Se aplicará autenticación multifactor en sistemas críticos.
- **Trazabilidad:** Todas las acciones relacionadas con la gestión de accesos serán registradas y auditadas.

4. Responsabilidades

- **Área de TI:** Implementar y mantener los controles técnicos, realizar revisiones periódicas y conservar evidencias.
- **Custodios de Activos:** Validar la pertinencia de los accesos otorgados a usuarios bajo su responsabilidad.
- **Representantes del SGCS BASC:** Aprobar cambios en accesos críticos y supervisar el cumplimiento de esta política.

5. Procedimientos

- **Asignación de accesos:** Basada en roles definidos en la Matriz de Criticidad de Cargos.

- **Revisión periódica:** Trimestral para cargos críticos, semestral para cargos medios y anual para cargos de baja criticidad.
- **Registro y auditoría:** Mantener evidencias en el **Registro de Revisiones Periódicas de Accesos** y en los informes de auditoría.

6. Cumplimiento

El incumplimiento de esta política será considerado una falta grave y podrá derivar en sanciones conforme a las normativas internas y legales aplicables.

Versión	Fecha	Descripción	Responsable
1.0	_____	Emisión inicial	_____

M. Anexo: TI-INF-REG-02

Registro de Revisión Periódica de Accesos Empresa de Servicio Electrónicos

Código Documental: TI-INF-REG-02
Área Revisada: _____
Fecha de Revisión: _____
Responsable: _____
Periodo Evaluado: _____

Usuario	Cargo	Rol Asignado	Permisos Actuales	Resultado de la Revisión	Acciones Correctivas	Fecha de Ejecución	Firma Responsable

N. Anexo: TI-LAC-POL-01

POLÍTICA DE LICENCIAMIENTO Y ACTUALIZACIÓN DE LA EMPRESA DE SERVICIOS ELECTRÓNICOS

Código: TI-LAC-POL-01
Versión: 1.0
Fecha de Emisión: ___ / ___ / ____
Aprobación: Gerencia General

1. Objetivo

Establecer los lineamientos para garantizar el uso exclusivo de hardware y software licenciados y actualizados en la organización, con el fin de proteger la infraestructura tecnológica contra amenazas informáticas y cumplir con los requisitos del estándar BASC y las mejores prácticas internacionales.

2. Alcance

Esta política aplica a todos los sistemas, aplicaciones, equipos y dispositivos tecnológicos utilizados por la organización, incluyendo servidores, estaciones de trabajo, software corporativo y herramientas de seguridad.

3. Principios

- **Legalidad:** Todo software debe contar con licencia vigente y cumplir con las disposiciones legales.
- **Actualización continua:** Se deben aplicar parches de seguridad y actualizaciones en plazos definidos para reducir vulnerabilidades.
- **Control documental:** Mantener registros actualizados de licencias, fechas de vencimiento y estado de actualización.
- **Protección integral:** Implementar mecanismos de seguridad complementarios como antivirus, firewalls y cifrado.

4. Responsabilidades

Área de TI:

- Mantener el inventario actualizado de hardware y software licenciados.
- Verificar la vigencia de licencias y aplicar actualizaciones periódicas.
- Documentar las revisiones en el **Registro de Verificación Periódica**.

Representantes del SGCS BASC:

- Supervisar el cumplimiento de esta política y aprobar renovaciones críticas.

5. Procedimientos

- **Inventario de Licencias:** Registrar todos los activos tecnológicos en la **Matriz De Criticidad de Activos**.
- **Revisión Periódica:** Realizar verificaciones trimestrales para sistemas críticos y semestrales para el resto, documentando hallazgos y acciones correctivas.

- **Evidencia Documental:** Conservar registros de inventario, revisiones y actualizaciones para auditorías BASC.

6. Cumplimiento

El incumplimiento de esta política será considerado una falta grave y podrá derivar en sanciones conforme a las normativas internas y legales aplicables.

Versión	Fecha	Descripción	Responsable
1.0	_____	Emisión inicial	_____

O. Anexo TI-LAC-REG-01

REGISTRO DE VERIFICACIÓN DE LICENCIAS Y ACTUALIZACIONES

Código del Documento: TI-LAC-REG-01
Versión: 1.0
Fecha de emisión: ____ / ____ / _____
Área responsable: Analista de TI

1. Datos Generales del Sistema

Ítem	Descripción
Nombre del sistema	
Tipo de activo	Software / Sistema Operativo / Aplicación / Herramienta de Seguridad / Otro
Proveedor / Fabricante	
Responsable del activo	
Ubicación (servidor/estación)	
Número de licencia / Serial / ID de activación	
Tipo de licencia	Perpetua / Suscripción / OEM / Enterprise / Otro
Fecha de adquisición	
Fecha de expiración (si aplica)	

2. Verificación de Licenciamiento

Fecha de revisión	Estado de licencia	Evidencia revisada	Hallazgos	Cumple	Responsable
	Vigente / Expirada / No localizada / En riesgo	Captura, documento, factura, portal		Sí / No	

3. Verificación de Actualizaciones

Fecha de revisión	Versión instalada	Última versión disponible	Tipo de actualización	Acción realizada	Evidencia	Responsable

			Seguridad / Funcional / Crítica	Actualizado / Pendiente / Programado	Captura / Log	

4. Requerimientos y Acciones Correctivas

Nº	Descripción del hallazgo	Riesgo	Acción correctiva	Responsable	Fecha compromiso	Estado
1		Bajo / Medio / Alto				Pendiente / En proceso / Cerrado

5. Observaciones Generales

_____

_____

_____

6. Firma de Conformidad

Rol	Nombre	Firma	Fecha
Analista TI			
Representantes SGCS-BASC			

P. Anexo: TI-CCS-POL-05

POLÍTICA DE CAPACITACIÓN Y CONCIENTIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA DE SERVICIOS ELECTRÓNICOS

Código sugerido: TI-CCS-POL-05
Versión: 1.0
Aprobado por: Gerencia General
Vigencia: ___ / ___ / _____

1. Objetivos

Promover una cultura organizacional basada en la seguridad, el cumplimiento normativo y la prevención de riesgos, asegurandeo que el personal conozca los requisitos BASC vinculados a su rol y de esta forma reducir incidentes derivados de acciones humanas, errores, desconocimiento o falta de conciencia lo que garantiza que el personal entienda sus responsabilidades en el tratamiento seguro de la información, con la finalidad de proveer lineamientos para la ejecución del Plan Anual de Capacitación en Seguridad de la Información.

2. Alcance

Esta política aplica a todo el personal interno, independiente de su modalidad, al personal externo que tenga acceso a información, sistemas o instalaciones, personal de proveedores críticos o aliados estratégicos que interactúen con activos de información y nuevos ingresos y pasantes, previo a la asignación de accesos.

3. Bases normativas

Esta política se fundamenta en:

- **Estándar BASC V6** – Controles de Seguridad y Gestión del Talento Humano (Cap. 5.3, 6.4 y otros específicos).
- **ISO/IEC 27001:2022** — Cláusula 7.2 (Competencia) y 7.3 (Concientización).
- **ISO/IEC 27002:2022** — Control 6.3 (Concientización, educación y formación en seguridad).
- Legislación nacional respecto a gestión de datos, privacidad y seguridad digital.

4. Principios de la política

La organización establece que:

4.1. Todo el personal debe recibir capacitación formal en Seguridad de la Información como requisito para el cumplimiento BASC y para garantizar el manejo seguro de los activos informáticos.

4.2. La capacitación deberá realizarse de forma anual, periódica y obligatoria, incluyendo:

- Inducción inicial
- Cursos generales para todo el personal
- Formación específica para roles críticos

- Actualizaciones cuando existan cambios tecnológicos, amenazas emergentes o incidentes relevantes.

4.3. Todos los usuarios deben mantener un nivel de conciencia adecuado respecto a:

- Buenas prácticas digitales
- Gestión adecuada de contraseñas y accesos
- Uso responsable de sistemas, dispositivos y servicios tecnológicos
- Identificación y reporte de amenazas como phishing, malware, ingeniería social
- Política de uso aceptable y políticas asociadas de TI

4.4. Las asistencias, evaluaciones, simulaciones y métricas deben quedar registradas y documentadas como evidencia del cumplimiento del SGCS BASC.

4.5. Ningún usuario recibirá credenciales o permisos de acceso mientras no haya completado la inducción obligatoria.

4.6. El incumplimiento de la capacitación será considerado una no conformidad y podrá sujetarse a acciones disciplinarias internas de acuerdo con el Reglamento Interno de Trabajo.

4.7. El área de Tecnología, en conjunto con el Oficial de Seguridad, deberá:

- Elaborar un plan anual de formación
- Ejecutar simulaciones de phishing y ejercicios de concientización
- Mantener los anexos y registros oficiales del procedimiento
- Evaluar periódicamente la eficacia del programa

5. Responsabilidades

Gerencia General

- Aprobar la política y garantizar recursos para su ejecución.

Representantes BASC

- Dirigir el programa de capacitación.
- Mantener vigentes los contenidos.
- Custodiar evidencias y reportes hacia auditorías.

Área de TI

- Proveer contenidos técnicos, simulaciones, evaluaciones y soporte operativo.
- Garantizar que ningún usuario obtenga acceso sin capacitación inicial.

Talento Humano

- Gestionar la matrícula y seguimiento del personal.
- Integrar la capacitación en los procesos de inducción.

Colaboradores

- Participar obligatoriamente en la formación.
- Aplicar lo aprendido en su labor diaria.
- Reportar situaciones sospechosas o incidentes.

6. Revisión y Actualización

Esta política será revisada de manera anual, o antes si existieran cambios relevantes en la infraestructura tecnológica, en los requisitos BASC o en los riesgos asociados al uso de dispositivos externos.

Versión	Fecha	Descripción	Responsable
1.0	_____	Emisión inicial	_____

Q. Anexo: TI-CCS-PR-05

PROCEDIMIENTO DE CAPACITACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA DE SERVICIOS ELECTRÓNICOS

Código: TI-CSS-PR-01
Versión: 1.0
Fecha: *[dd/mm/aaaa]*
Aprobado por: Gerencia General

1. Objetivo

Establecer el proceso formal para planificar, ejecutar, evaluar y documentar las actividades de capacitación y sensibilización del personal en materias relacionadas con la seguridad de la información, en conformidad con los requisitos del estándar **WBO BASC** y en alineación con las buenas prácticas establecidas en **ISO/IEC 27001:2022**, particularmente en los controles relativos a concientización (Anexo A – Control 6.3).

2. Alcance

Este procedimiento aplica a todos los colaboradores, contratistas, proveedores con acceso a información o sistemas, y personal temporal vinculado a procesos operativos, administrativos o tecnológicos de la organización.

3. Referencias Normativas

- **WBO BASC – Estándares Internacionales de Seguridad** (versión vigente).
- **ISO/IEC 27001:2022**, Sistema de Gestión de Seguridad de la Información.
- **ISO/IEC 27002:2022**, guía de controles de seguridad.
- *Von Solms & Van Niekerk (2013). "From information security to cyber security." Computers & Security.*
- *SANS Institute Security Awareness Report (anual).*
- *Peltier, T. (2016). Information Security Policies, Procedures and Standards.*

4. Definiciones

- **Capacitación:** Actividad formal orientada a desarrollar competencias técnicas.
- **Sensibilización:** Actividad breve orientada a generar consciencia y modificar comportamientos.
- **Participante:** Persona obligada a recibir formación.
- **SGCS BASC:** Sistema de Gestión en Control y Seguridad.

5. Responsabilidades

Rol	Responsabilidad
Dirección	Aprobar el programa anual de capacitación.
Responsables BASC	Elaborar el plan anual, definir temarios, coordinar sesiones y registrar evidencias.
TI	Apoyar con contenidos técnicos y reportes de incidentes a incluir en la formación.
Talento Humano	Gestionar convocatorias, asistencia y almacenamiento de registros.
Colaboradores	Participar activamente y aplicar lo aprendido en su trabajo diario.

6. Procedimiento

6.1. Planificación anual

1. El Oficial de Seguridad elabora el **Plan Anual de Capacitación de Seguridad** basado en:
    - Análisis de riesgos.
    - Controles BASC aplicables.
    - Requisitos ISO/IEC 27001.
    - Resultados de auditorías internas/externas.
    - Incidentes o brechas de seguridad ocurridas.
2. El plan debe incluir:
    - Objetivos de formación.
    - Temas y contenidos.
    - Responsables.
    - Fechas y modalidad.
    - Indicadores de desempeño.
3. La Dirección revisa y aprueba el plan.

6.2. Diseño de contenido

El contenido incluirá, como mínimo:

- Políticas y procedimientos BASC.
- Manejo de información sensible.
- Buenas prácticas de contraseñas y autenticación.
- Reconocimiento de correos maliciosos (phishing).
- Uso seguro de dispositivos y aplicaciones.
- Reporte de incidentes de seguridad.
- Actualizaciones normativas relevantes.

6.3. Ejecución de la capacitación

1. Las sesiones pueden ser:
    - Presenciales.
    - Virtuales sincrónicas.
    - Asincrónicas (e-learning).
    - Microcapsulas de sensibilización mensuales.
2. Todo participante debe registrar asistencia mediante lista o sistema electrónico.
3. Se realizarán ejercicios prácticos cuando aplique, tales como:
    - Simulaciones de phishing.
    - Prácticas de respuesta ante incidentes.
    - Pruebas de uso seguro de sistemas.

6.4. Evaluación del aprendizaje

1. Se aplican evaluaciones posteriores mediante cuestionario o prueba práctica.

2. Se establece un **mínimo del 80% de aprobación**.
3. Participantes que no aprueben deberán repetir la capacitación.
4. Se registran resultados en el Sistema de Gestión BASC.

6.5. Registro y documentación

Se deben mantener archivados como evidencia BASC:

- Plan Anual de Capacitación.
- Materiales utilizados.
- Listas de asistencia.
- Evaluaciones y resultados.
- Reportes de simulaciones o ejercicios.
- Acciones correctivas derivadas (si aplican).

Los registros se conservan mínimo **3 años**.

6.6. Mejora continua

Se realiza una revisión anual considerando:

- Retroalimentación de participantes.
- Análisis de incidentes de seguridad.
- Hallazgos de auditorías.
- Cambios normativos BASC o ISO.

Las mejoras se integran al nuevo plan anual.

7. Indicadores

- % de colaboradores capacitados vs total.
- % de aprobación por curso.
- Nº de incidentes atribuibles a error humano (tendencia).
- Resultados de pruebas de phishing controlado.

8. Anexos

- Anexo 1: Formato – Plan Anual de Capacitación.
- Anexo 2: Lista de Asistencia.
- Anexo 3: Evaluación de Conocimientos.
- Anexo 4: Informe de Simulaciones de Phishing.

FORMATO: PLAN ANUAL DE CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN
Código: TI- CSS -FR-01
Versión: 1.0
Año: _____
Responsable: Representantes BASC

Elemento	**Descripción**
Objetivo general	_____
Objetivos específicos	_____
Normativas aplicables	BASC, ISO/IEC 27001, ISO/IEC 27002, políticas internas
Riesgos asociados que motivan la capacitación	_____
Temas / Módulos	_____
Público objetivo	_____
Modalidad (presencial, virtual, e-learning)	_____
Frecuencia	Mensual / Trimestral / Semestral / Anual
Fechas programadas	_____
Responsable del contenido	_____
Responsable de ejecución	_____
Indicadores asociados (KPI)	% de participación, % de aprobación, reducción de incidentes

Aprobación:
Firma Dirección: _____
Fecha: ___ / ___ / _____

FORMATO: LISTA DE ASISTENCIA

Código: TI- CSS-FR-02

Capacitación: _____

Fecha: ___ / ___ / _____

Facilitador: _____

Nº	Nombre del participante	Cargo / Área	Tipo de personal (interno / externo)	Firma / Confirmación
1				
2				
3				
…				

Observaciones del facilitador:

_____
_____

_____
_____

FORMATO: EVALUACIÓN DE CONOCIMIENTOS
Código: TI-CSS-FR-03
Capacitación: _____
Fecha: ___ / ___ / _____
Participante: _____
Área: _____
Instrucciones
Responda correctamente todas las preguntas. Puntaje mínimo de aprobación: **80%**.

1. Preguntas de opción múltiple

1. ¿Qué debe hacer un usuario si detecta un correo sospechoso?
   - ☐ A. Ignorarlo
   - ☐ B. Reportarlo inmediatamente al Oficial de Seguridad
   - ☐ C. Abrirlo para verificar su contenido
   - ☐ D. Reenviarlo a otros compañeros

2. ¿Cuál es la longitud mínima recomendada para una contraseña segura?
   - ☐ A. 4 caracteres
   - ☐ B. 6 caracteres
   - ☐ C. 8 o más caracteres
   - ☐ D. No importa la longitud

3. El phishing se define como:
   - ☐ A. Un ataque físico al servidor
   - ☐ B. Un método para engañar a usuarios y obtener información
   - ☐ C. Un proceso de respaldo
   - ☐ D. Una auditoría BASC

(Puedes pedirme que genere 10, 20 o más preguntas si lo necesitas.)

2. Preguntas abiertas

1. Explique brevemente qué es un incidente de seguridad.

_____
_____

2. ¿Qué acciones debe realizar antes de compartir información sensible?

_____
_____

3. Mencione tres buenas prácticas de seguridad en el uso diario de sistemas.

_____
_____
_____
_____

Resultado final

Ítem	**Resultado**
Puntaje total	_____ %

¿Aprobado?	Sí / No
Fecha de retroalimentación	___ / ___ / _____

Firma Evaluador: _____

FORMATO: INFORME DE SIMULACIÓN DE PHISHING
Código: TI-CSS-FR-04
Fecha: ___ / ___ / _____
Responsable del ejercicio: Analista TI
Tipo de simulación: Phishing / Smishing / Vishing / Mixto
Población objetivo: _____

1. Objetivo del ejercicio

_____
_____

2. Descripción del escenario

- Plantilla utilizada: _____
- Tipo de mensaje señuelo: _____
- Temática utilizada (ej. actualización de contraseña, premio, alerta bancaria, etc.): _____

3. Resultados del ejercicio

Métrica	**Resultado**
Total de usuarios incluidos	_____
Usuarios que abrieron el correo	_____
Usuarios que hicieron clic en enlace	_____
Usuarios que entregaron credenciales (simulado)	_____
Usuarios que reportaron correctamente el intento	_____
Porcentaje de riesgo general	_____ %

4. Análisis y hallazgos

_____
_____
_____
_____

5. Acciones correctivas y preventivas

- Capacitación adicional a áreas críticas
- Ajustes al contenido de concientización
- Reforzamiento de controles técnicos
- Otras acciones: _____

6. Conclusiones

_____
_____
_____

Firma responsable TI: _____
Firma Representante BASC: _____

R. Anexo: TI-GSU-POL-01

POLITICA DE GESTIÓN DE SUPERUSUARIOS Y CONTINUIDAD DE CREDENCIALES DE LA EMPRESA DE SERVICIOS ELECTRÓNICOS

Código sugerido: TI-GSU-POL-01
Versión: 1.0
Aprobado por: Gerencia General
Fecha: ___ / ___ / _____

1. Objetivo

Establecer lineamientos para la administración segura de cuentas con privilegios elevados (superusuarios), garantizando la continuidad de credenciales únicamente en equipos activos cuando sea estrictamente necesario, conforme a BASC.

2. Alcance

Aplica a todos los sistemas críticos, plataformas tecnológicas y cuentas privilegiadas utilizadas en la infraestructura de la organización.

3. Principios de la Política

La organización establece que las cuentas de superusuario estarán sujetas a controles estrictos de administración, monitoreo y auditoría.
La continuidad de credenciales será permitida únicamente bajo justificación operacional documentada y aprobación formal del área de Gerencia General.
Toda acción relacionada con credenciales privilegiadas deberá ser trazable, registrada en sistemas de auditoría y cumplir con los principios de temporalidad controlada y autorización formal.
Se aplicarán mecanismos de autenticación robusta y monitoreo continuo.

4. Responsabilidades

Gerencia General
Aprobar la política y asignar recursos financieros, tecnológicos y humanos requeridos para su el cumplimiento
Área de TI
Administración de cuentas, implementación técnica, monitoreo y mantenimiento de controles.
Representantes del SGCS BASC
Aprobación de excepciones, verificación de cumplimiento y reportar observaciones.

5. Cumplimiento

Las acciones correctivas derivadas serán gestionadas de acuerdo con los procedimientos internos del sistema de gestión, asegurando su seguimiento hasta su implementación total. Esta política es de cumplimiento obligatorio para todas las áreas involucradas y constituye un elemento esencial para fortalecer la seguridad tecnológica y la continuidad operativa de la organización.

Versión	Fecha	Descripción	Responsable
1.0	_____	Emisión inicial	_____

S. Anexo: TI-GSU-PR-01

PROCEDIMIENTO DE CONTROL A SUPERUSUARIOS Y CONTINUIDAD DE CREDENCIALES DE LA EMRPESA DE SERVICIOS ELECTRÓNICOS

Código sugerido: TI-GSU-PR-01
Versión: 1.0
Aprobado por: Gerencia General
Fecha: ___ / ___ / _____

1. Objetivo

Establecer los pasos para gestionar cuentas privilegiadas garantizando la continuidad segura de credenciales en equipos activos y la continuidad operativa en escenarios críticos mediante la preservación temporal de credenciales privilegiadas, bajo autorización formal y registro en bitácora, minimizando riesgos de seguridad

2. Alcance

Aplica a todos los sistemas críticos y cuentas con privilegios elevados en la infraestructura tecnológica de la organización.

3. Procedimiento Operativo

Se detalla los pasos que se deben cumplir para este procedimiento:

3.1. Identificación y Clasificación

Inventariar todas las cuentas de superusuario y asociarlas a sistemas críticos.

3.2. Validación de Necesidad

Confirmar si la continuidad de credenciales es indispensable para la operación.

3.3. Autorización Formal

Solicitar aprobación documentada a Gerencia General.

3.4. Implementación de Controles

Aplicar rotación segura de contraseñas, autenticación multifactor y registro en sistemas de auditoría.

3.5. Monitoreo y Reporte

Supervisar el uso de credenciales y generar reportes periódicos para revisión por los Representantes del SGCS BASC

3.6. Revisión y Revocación

Evaluar la vigencia de la continuidad cada 30 días y revocar credenciales cuando ya no sean necesarias.

4. Activación de Contingencia para Preservación Temporal de Credenciales

Se establecen los escenarios en los que se debe activar la contingencia

- Fallo crítico en sistemas que impida la rotación inmediata de credenciales.
- Interrupción de procesos operativos esenciales que requieran acceso privilegiado continuo.
- Emergencias tecnológicas donde la revocación inmediata comprometa la operación.

5. **Procedimiento de Contingencia Preservación Temporal de Credenciales**

1) Detección del escenario crítico

El área de TI Identifica la situación que requiere continuidad temporal de credenciales ajustándose a lo establecido en el apartado anterior.

2) Solicitud de activación

El Analista TI comunica la necesidad a los Encargados BASC y a Gerencia General.

3) Autorización formal

Los Encargados BASC aprueban la activación mediante registro en el formato de contingencia.

4) Registro en bitácora

Se documenta: motivo, cuentas afectadas, fecha/hora de activación, responsables.

5) Aplicación de controles adicionales

Activar monitoreo intensivo de las cuentas en uso y limitar el acceso solo al personal autorizado.

6) Revocación inmediata

Una vez superada la contingencia, se revocan las credenciales preservadas y se ejecuta la rotación segura.

7) Informe post-evento

Encargados BASC generan un reporte para auditoría interna y lo archiva en el sistema documental.

6. **Responsabilidades**

Gerencia General
Aprobar el procedimiento y asignar recursos financieros, tecnológicos y humanos requeridos para su el cumplimiento

Área de TI
Administración de cuentas, implementación técnica, monitoreo y mantenimiento de controles.

Representantes del SGCS BASC
Aprobación de excepciones, verificación de cumplimiento y reportar observaciones.

Versión	Fecha	Descripción	Responsable
1.0	_____	Emisión inicial	_____

T. Anexo: TI-SIM-POL-01

POLÍTICA DE SIMULACROS Y EJERCICIOS PRÁCTICOS DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA DE SERVICIOS ELECTRÓNICOS

Código sugerido: TI-SIM-POL-01
Versión: 1.0
Aprobado por: Gerencia General
Fecha: ___ / ___ / _____

7. Objetivo

La empresa establece esta política con el propósito de fortalecer su capacidad de respuesta ante incidentes de seguridad y validar la eficacia de los controles implementados en su infraestructura tecnológica. Con ello se garantiza el cumplimiento de los requisitos del estándar BASC y el mejoramiento continuo del Sistema de Gestión de Seguridad.

8. Alcance

La empresa se compromete a planificar, ejecutar y documentar simulacros y ejercicios prácticos de seguridad de la información de manera periódica, asegurando que estas actividades permitan verificar la eficiencia de los procedimientos establecidos, evaluar el nivel de preparación del personal, identificar vulnerabilidades operativas y determinar la capacidad de recuperación ante posibles incidentes tecnológicos.

9. Principios de la Política

La empresa realizará de manera planificada y periódica los siguientes tipos de simulacros relacionados con las tecnologías de la información:

Simulacro de Respuesta a Incidentes de Seguridad:
Ejercicio orientado a evaluar la capacidad del personal para identificar, contener, comunicar y resolver incidentes de ciberseguridad conforme a los procedimientos vigentes.

Simulacro de Recuperación ante Desastres Tecnológicos (DRP):
Actividad que permitirá validar la operatividad del plan de recuperación, medir tiempos de restablecimiento, verificar la disponibilidad de respaldos y confirmar la funcionalidad de los sistemas críticos tras un evento disruptivo.

Simulacro de Pérdida o Exposición de Información:
Escenario diseñado para medir el proceso de notificación, análisis de impacto, aplicación de medidas de mitigación y activación de controles en situaciones de fuga, pérdida o acceso no autorizado a información.

Simulacro de Caída o Interrupción de Servicios Críticos:
Ejercicio que evalúa la capacidad de respuesta ante fallas en servidores, redes, sistemas de comunicación o aplicaciones esenciales para la operación.

Ejercicios de Ingeniería Social y Educación en Seguridad:
Simulaciones controladas dirigidas a evaluar la conciencia del personal frente a correos fraudulentos, accesos no autorizados, solicitudes sospechosas o técnicas comunes de manipulación.

10. Responsabilidades

Todos los simulacros deberán ser planificados por el Analista de TI y ejecutados conforme a un cronograma anual aprobado por la Gerencia General. Cada simulacro deberá documentarse, incluir objetivos, alcance, responsables, metodología y criterios de evaluación. Los resultados serán registrados formalmente, incorporando hallazgos, desviaciones, evidencias y oportunidades de mejora.

11. Cumplimiento

Las acciones correctivas derivadas serán gestionadas de acuerdo con los procedimientos internos del sistema de gestión, asegurando su seguimiento hasta su implementación total. Esta política es de cumplimiento obligatorio para todas las áreas involucradas y constituye un elemento esencial para fortalecer la seguridad tecnológica y la continuidad operativa de la organización.

Versión	Fecha	Descripción	Responsable
1.0	_____	Emisión inicial	_____