UNIVERSIDAD GERARDO BARRIOS.

INGENIERÍA EN SISTEMAS Y REDES INFORMÁTICAS.

FACULTAD DE CIENCIA Y TECNOLOGÍA.

EMPRESA:

FLERT SALON & SPA

TEMA:

APLICACIÓN DE COBIT 5.0

DOCENTE:

LICDO. ARMANDO FEDERICO VENTURA GUEVARA.

INTEGRANTES:

JAVIER EDGARDO MEJÍA RODRÍGUEZ.

FÁTIMA DEL CARMEN AYALA SANTOS.

FERNANDO RUBÉN CHÉVEZ SÁNCHEZ.

SAN MIGUEL, DICIEMBRE 2024.

INDÍCE

INTRODUCCIÓN.

En el capítulo I en donde se presenta la Información institucional de "FLERT SALON & SPA" que proporciona un entendimiento integral de la empresa, desde su historia hasta su organización interna. Se analizan aspectos claves como Misión, Visión y Valores de la empresa que definen su identidad y su dirección estratégica, también se describen áreas funcionales y el papel que juega la TI dentro de la organización, destacando la importancia de este en el funcionamiento diario y el cumplimento de los objetivos de la empresa. Al finalizar se realiza y se presenta un análisis FODA realizado tanto a la empresa como a la unidad TI, proporcionando un marco para entender las oportunidades y los retos que la empresa enfrenta a lo largo de su camino.

En el capítulo II llamado estado del arte encontrará el desarrollo sobre las generalidades de la metodología COBIT 5.0 el cuál abarca una introducción al marco de trabajo dónde encontrará beneficios y logros que se obtienen de aplicar esta metodología, también se desarrolla el propósito que tiene COBIT 5.0, además de encontrar a detalle cada uno de los principios con los que cuenta está metodología. Se observará el modelo de gobierno de la empresa, detalla el nivel de madurez con respecto a TI y, por último, se subraya la importancia del manejo de TI en las empresas para mejorar la eficiencia, seguridad y cumplimientos normativos.

En el capítulo III se aborda el desarrollo de una auditoría en el área de informática de la empresa Flert Salon & Spa, utilizando la metodología COBIT 5.0. A lo largo de este capítulo, se definirán de manera clara y detallada los elementos esenciales de la auditoría, comenzando por los objetivos y el alcance, los cuales reflejan las metas específicas que se buscan alcanzar en el proceso de auditoría. Asimismo, se describirá la metodología de trabajo que guiará cada una de las etapas del proceso, garantizando una

evaluación exhaustiva y sistemática. También se determinarán los recursos necesarios, tanto humanos como financieros y tecnológicos, para llevar a cabo la auditoría de manera eficiente. Además, se detallará el tiempo estimado para la implementación de cada fase del proyecto, con el fin de asegurar una ejecución efectiva y oportuna. Finalmente, se identificarán las necesidades y expectativas de las partes interesadas de Flert Salon & Spa mediante un instrumento de 22 preguntas de esta forma estamos reconociendo que su participación y compromiso son clave para el éxito de la auditoría.

El Capítulo IV aborda de manera integral la implementación de procesos clave que garantizan la gestión y optimización de riesgos y la seguridad dentro de Flert SALON & SPA, tomando como base las mejores prácticas establecidas en el marco COBIT 5.0. Este capítulo desarrolla las estrategias necesarias para cumplir con los objetivos de los procesos EDM03 (Asegurar la optimización del riesgo), APO12 (Gestionar el riesgo) y APO13 (Gestionar la seguridad), proporcionando un enfoque estructurado para identificar, analizar y mitigar riesgos operativos y de TI, al tiempo que se asegura la protección de los activos de información y la continuidad del negocio. Cada uno de estos procesos es fundamental para establecer una gobernanza eficiente, minimizar las amenazas y mejorar la resiliencia organizacional, todo esto alineado con los objetivos estratégicos de la empresa.

OBJETIVOS.

OBJETIVO GENERAL.

- Optimizar la gobernanza y gestión de las tecnologías de la información en 'FLERT SALON & SPA' para alinear las prácticas del departamento de TI con los objetivos estratégicos de la empresa.

OBJETIVOS ESPECÍFICOS.

- Examinar y valorar la efectividad de los procesos de gestión de riesgos de TI implementados en la organización de "FLERT SALON & SPA", mediante el análisis de la identificación, evaluación, mitigación y monitoreo de riesgos, con el fin de determinar su alineación con los estándares de COBIT 5.0
- Evaluar los sistemas y procesos de TI en "FLERT SALON & SPA" para identificar oportunidades de mejora en la seguridad de la información, optimización de recursos, y cumplimiento de normativas, con el fin de fortalecer su apoyo a los objetivos estratégicos de la empresa.

ALCANCES.

- Analizar cómo "FLERT SALON & SPA" gestiona su infraestructura tecnológica, incluyendo sistemas de reservas, manejo de bases de datos de clientes, y plataformas de pago. Esto implica evaluar la eficiencia de sus sistemas de TI en términos de seguridad, disponibilidad, y alineación con los objetivos del negocio.
- Evaluar cómo la tecnología está siendo utilizada para optimizar los procesos operativos del salón, como la gestión de citas, el control de inventarios, y la atención al cliente. Identificar áreas donde la automatización o mejoras tecnológicas pueden aumentar la eficiencia.

- Revisar si "FLERT SALON & SPA" cumple con las regulaciones locales y estándares de la industria en cuanto al manejo de datos, transacciones electrónicas, y protección de la privacidad de los clientes. Asegurarse de que la empresa minimiza riesgos legales mediante la correcta implementación de políticas de TI.

LIMITANTES.

- La poca disponibilidad de datos y el acceso a la información interna de la empresa, la calidad de la auditoria se verá afectada si la información proporcionada está incompleta o debido a las políticas internas de la empresa o por restricciones de seguridad, incluso por falta de documentación la información no es proporcionada.
- El tiempo asignado para realizar la auditoria nos podría restringir la posibilidad de hacerla de manera exhaustiva, ya que COBIT 5.0 abarca detalladamente las áreas de TI y el tiempo limitado podría forzar a priorizar ciertos procesos sobre otros, lo que podría resultar en una evaluación menos completa.

CAPITULO I – INFORMACIÓN INSTITUCIONAL.

1.1 RECONOCIMIENTO DE LA EMPRESA.

1.1.1 NATURALEZA DE LA EMPRESA: Comercial.

1.1.2 NOMBRE DE LA EMPRESA: FLERT Salon & Spa

1.1.3 DIRECCIÓN: CENTRO COMERCIAL METROCENTRO SAN MIGUEL, LOCAL 13E Y 89E.

1.1.4 SITIO WEB: Elite Brands S.A de C.V & https://flert.com.sv/

1.2 RESEÑA HISTORICA DE LA EMPRESA.

Somos una distribuidora basada en El Salvador con más de 30 años de experiencia, cubriendo todos los canales de distribución de cuidado personal y consumo.

Somos una de las cadenas de salones de belleza más grande de El Salvador. Contamos con cuatro áreas de servicio y venta: servicio de salón, servicios de cabina, producto profesional y perfumería. Nos encontramos en expansión y contamos con un equipo de más de 80 profesionales de belleza con altos estándares técnicos y de atención al cliente.

En marzo de 2020, en cumplimiento con las medidas sanitarias del gobierno durante la pandemia de COVID 19, FLERT cerró temporalmente todos sus salones de belleza, cabinas y tiendas de productos. Esto implicó una interrupción significativa en los ingresos debido a la suspensión de servicios presenciales.

Para abril de 2020, FLERT aceleró la implementación de su plataforma de comercio electrónico para la venta de productos profesionales y de perfumería. Esta medida permitió a la empresa mantener el contacto con sus clientes y generar ingresos mediante la venta en línea de productos para el cuidado personal en casa.

Durante la cuarentena, FLERT implementó programas de formación en línea para capacitar a su equipo en las últimas tendencias de belleza y normativas de bioseguridad. Esta iniciativa aseguró que el personal estuviera preparado para la reapertura y brindara un servicio seguro y de calidad.

Tras meses de cierre, FLERT reabrió sus salones bajo estrictas medidas sanitarias, asegurando la protección de clientes y colaboradores. La empresa relanzó sus servicios presenciales con nuevas políticas de reserva en línea para controlar la afluencia y evitar aglomeraciones.

1.3 ELEMENTOS DEL PLAN ESTRATEGICO DE LA EMPRESA.

1.3.1 MISIÓN.

Desarrollar, brindar el mejor servicio y consolidar marcas reconocidas a nivel mundial, a través de nuestra cobertura nacional, fuerza de ventas y alianzas comerciales estratégicas.

1.3.2 VISIÓN.

Consolidarnos como la mejor empresa de distribución en la región. Ser la mejor opción como socio comercial para nuestros fabricantes y clientes.

1.3.3 VALORES.

Al revisar su página y al hacer una investigación en la empresa no encontramos que cuentan con valores por lo que se proponen los siguientes:

- **Desarrollo:** Estamos comprometidos con el desarrollo y la consolidación de las marcas que representamos. Nos esforzamos por fortalecer su presencia en el mercado salvadoreño, garantizando su crecimiento sostenible y éxito a largo plazo.
- **Calidad:** Nuestro objetivo es ofrecer un servicio de calidad excepcional. A través de nuestra cobertura nacional y alianzas

estratégicas, aseguramos que nuestros clientes reciban productos y servicios que superen sus expectativas, manteniendo siempre los más altos estándares de satisfacción.

- **Excelencia:** Nos dedicamos a alcanzar la excelencia en todos los aspectos de operación. Nuestro enfoque está en ofrecer productos y servicios de alta calidad que no solo satisfacen, sino que superan las expectativas de nuestros clientes y socios comerciales.

1.3.4 OBJETIVOS ESTRATEGICOS DE LA EMPRESA.

Al revisar su página y al hacer una investigación en la empresa no encontramos que cuentan con objetivos estratégicos por lo que se proponen los siguientes:

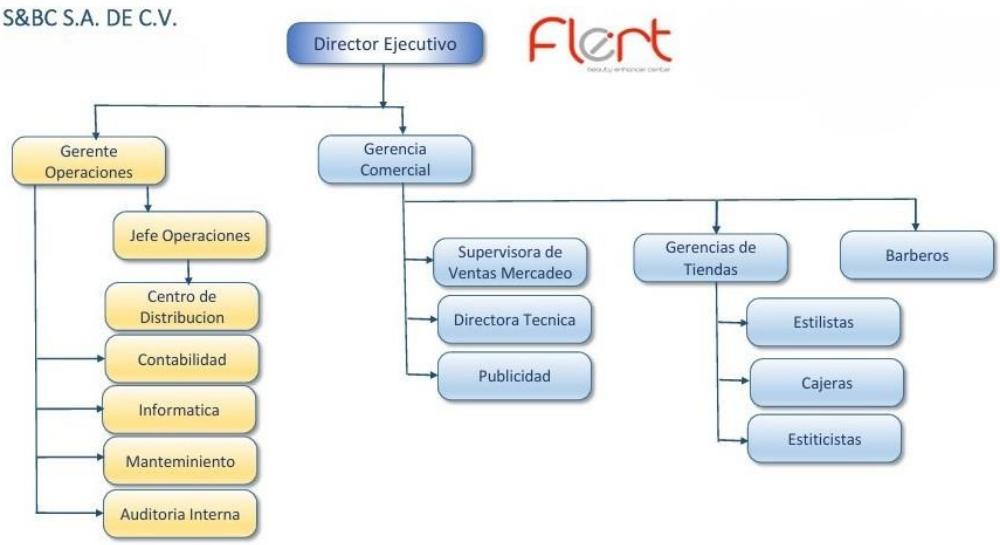
- **Consolidación de Marcas**: Fortalecer y expandir la presencia de marcas reconocidas a nivel mundial en la región.
- **Expansión de Cobertura:** Asegurar una cobertura nacional efectiva para sus productos y servicios.
- **Excelencia Operativa**: Ser la opción líder en distribución para fabricantes y clientes, ofreciendo servicios de alta calidad.
- **Alianzas Estratégicas:** Desarrollar y mantener alianzas comerciales clave para potenciar el crecimiento y la competitividad en el mercado.

1.3.5 DESCRIPCIÓN DE LOS SERVICIOS OFRECIDOS POR LA EMPRESA.

TIPO DE SERVICIO	DESCRIPCIÓN
Servicio de Salón	Incluye actividades relacionadas con el cuidado del cabello, como cortes, peinados, coloración, tratamientos capilares, y alisados.
Servicio de Cabina	Ofrecen tratamientos especializados para el cuidado de

	la piel y el cuerpo. Los servicios incluyen faciales, exfoliaciones, masajes relajantes, y tratamientos corporales para la reducción de medidas o mejora de la circulación.
Venta de Productos Profesionales	Pone a disposición de sus clientes una gama de productos profesionales para el cuidado del cabello y la piel. Estos productos están formulados con ingredientes de alta calidad y suelen ser los mismos que utilizan los estilistas y terapeutas en los tratamientos.
Venta de Perfumería	Ofrece una selección de perfumes y fragancias exclusivas y los clientes pueden elegir entre una variedad de marcas reconocidas.

1.4 JERARQUIA Y GOBERNABILIDAD DENTRO DE LA EMPRESA.



1.4.1 DESCRIPCIÓN DE LAS ÁREAS DE LA EMPRESA.

Área Principal	Sub-áreas	Descripción
Dirección Ejecutiva		Supervisión general y toma de decisiones estratégicas para la empresa.
Gerencia de Operaciones	Jefe de Operaciones	Coordinación de todas las operaciones diarias dentro de la empresa.
	Centro de Distribución	Gestión de inventarios y logística de distribución de productos a la tienda
	Contabilidad	Manejo de las finanzas, incluyendo cuentas por pagar y cobrar y la gestión de presupuestos.
	Informática	Soporte y gestión de la infraestructura tecnológica, incluyendo software y hardware.

	Mantenimiento	Supervisión y realización de tareas de mantenimiento preventivo y correctivo en las instalaciones.
	Auditoría Interna	Evaluar y asegurar la integridad de los procesos operativos y financieros.
Gerencia Comercial	Supervisora de Ventas y Mercado	Gestión de estrategias de ventas y marketing para aumentar la visibilidad y las ventas de la empresa.
	Directora Técnica	Aseguramiento de la calidad técnica de los servicios ofrecidos en el salón y spa.
	Publicidad	Desarrollo y ejecución de campañas publicitarias para promover la marca y los servicios.
Gerencia de Tiendas	Estilistas	Profesionales que ofrecen servicios de corte, coloración, peinados y otros cuidados capilares.
	Cajeras	Personal responsable del manejo de caja, transacciones y atención al cliente en el punto de venta.
	Esteticistas	Especialistas en tratamientos faciales, corporales y otros servicios de estética.
Área de Barbería		Servicios de barbería, incluyendo cortes de cabello y arreglos de barba para hombres.

1.5 DESCRIPCIÓN DEL AREA DE TECNOLOGÍA.

El área de tecnología en FLERT, se encarga de gestionar los sistemas operativos y de seguridad, desarrollar herramientas digitales, brindar soporte técnico, y analizar datos para optimizar la eficiencia y la experiencia del cliente.

1.5.1 POSICIONAMIENTO DE LA UNIDAD DE TI DENTRO DE LA EMPRESA.

La unidad de TI dentro del esquema de la organización se identifica como parte del área de Operaciones, reportando directamente al Gerente de Operaciones. Su misión y objetivo principal es garantizar el funcionamiento continuo y eficiente de la infraestructura tecnológica, ofreciendo soporte técnico, gestionando los sistemas de información y manteniendo la seguridad de los datos, para asegurar que todas las áreas de la empresa operen con tecnología alineada a los objetivos estratégicos de FLERT.

1.5.2 DESCRIPCIÓN DE PUESTOS DE LA UNIDAD DE TI.

CARGO	PERFIL
Anónimo Jefe de Unidad de TI	Ingeniero en Sistemas y Redes Informáticas.
Anónimo Encargado de soporte técnico.	Técnico en ingeniería en Sistemas y Redes Informáticas.

1.5.3 FUNCIONES Y ATRIBUCIONES DE LA UNIDAD DE TI.

ÁREA	TAREAS/RESPONSABILIDADES	DESCRIPCIÓN
Soporte	Brindar asistencia técnica y resolución de problemas.	Atender incidencias y asegurar la operatividad continua de los

		sistemas y equipos tecnológicos.
Seguridad	Implementar y mantener medidas de ciberseguridad.	Proteger los datos sensibles y garantizar la integridad de la información.
Infraestructura	Gestionar y mantener redes, servidores y equipos tecnológicos.	Gestionar y mantener redes, servidores y equipos tecnológicos.
Desarrollo	Diseñar e implementar nuevas aplicaciones o herramientas.	Desarrollar soluciones personalizadas para mejorar procesos internos.
Gestión de Proyectos	Coordinar e implementar proyectos tecnológicos.	Planificar y ejecutar proyectos de TI alineados con los objetivos de la empresa.
Capacitación	Formar al personal en el uso de herramientas tecnológicas.	Impartir talleres y entrenamientos para mejorar la competencia digital del equipo.

1.6 RECURSOS Y SISTEMAS DE INFORMACIÓN.

EQUIPO	AREA ASIGNADA	PERSONA ASIGNADA	CONTROLES ASIGNADOS	OBSERVACIONES
Desktop-9CI062K	Caja	Cenia López	Correctivo	El Windows no está activado.
Desktop-8BI073M	Atención al cliente	Merary Argueta	Correctivo	El Windows no está activado.

TIPO DE APLICACIÓN	NOMBRE DEL PROGRAMA	# DE LICENCIA	CARACTERISTICAS
Editor de Texto	Microsoft Word		Se utiliza para procesar información de la empresa.
Hoja de Cálculo	Microsoft Excel		Se utiliza para el análisis y gestión de datos financieros.
Presentaciones	Microsoft PowerPoint		Se emplea para la creación de presentaciones y material visual.
Escritorio Remoto	ANYDESK		Permite el acceso remoto para soporte técnico operaciones.
Base de Datos	TOAD FOR ORACLE		Herramienta para la gestión y consulta de bases de datos Oracle.
Lector de PDF	Adobe Acrobat Reader		Facilita la visualización y manejo de archivos PDF.
Navegador Web	Google Chrome		Navegador para la búsqueda de información y acceso a recursos.
Antivirus	ESET		Protección contra malware y amenazas cibernéticas.

TIPO DE RED	SEGURIDAD	ESTANDARES/CONTROLES
Anillo	Nivel 1	No se proporcionó la información

NOMBRE DEL SISTEMA DE INFORMACIÓN	AREAS Y PERSONA ASIGNADA	CONTROLES ASIGNADOS	RESPONSABLE DE SU MANTENIMIENTO
FLERT- Ventas	Caja - Cenia López	Control de acceso de inicio de sesión al sistema	Anónimo
Inventario	Gerencia- Sulma Cárcamo	Control de acceso de inicio de sesión al sistema	Anónimo

1.7 FODA DE LA EMPRESA

FORTALEZAS	OPORTUNIDADES
Amplia red de salones de belleza en El Salvador.	Expansión a nuevos mercados nacionales o internacionales.
Variedad de servicios y productos, desde salón y cabina hasta productos profesionales y perfumería.	Implementación de estrategias digitales y comercio electrónico para la venta de productos.
Reputación y reconocimiento en el mercado	Crecimiento del mercado de belleza y cuidado personal.
DEBILIDADES	**AMENAZAS**

Competencia en precios con otras cadenas de belleza y salones independientes.	Competencia creciente en el sector, tanto de cadenas como de salones pequeños.
Necesidad constante de capacitar al personal para mantener la calidad del servicio.	Cambios en las preferencias de los consumidores y tendencias de belleza.
Dependencia de tecnología y sistemas informáticos, lo que puede causar problemas si fallan.	Factores económicos externos que puedan afectar el poder adquisitivo de los clientes.

1.8 FODA DE LA UNIDAD DE TI.

FORTALEZAS	OPORTUNIDADES
Infraestructura tecnológica sólida para apoyar las operaciones de la empresa.	Implementación de tecnologías emergentes como la automatización y la inteligencia artificial.
Capacidad para desarrollar e implementar soluciones tecnológicas personalizadas.	Desarrollo de nuevas herramientas digitales que optimicen la experiencia del cliente.
Proceso eficiente de soporte técnico para asegurar la continuidad operativa.	Posibilidad de integrar nuevas plataformas de comercio electrónico y aplicaciones móviles.
DEBILIDADES	**AMENAZAS**
Recursos limitados para la rápida actualización de infraestructura y software.	Rápido avance tecnológico que pueda dejar obsoletas las soluciones actuales.

Falta de personal técnico suficiente en situaciones de alta demanda o proyectos grandes.	Ataques cibernéticos que comprometan la seguridad de la información de la empresa.
Dificultad para mantener al equipo constantemente actualizado con las últimas tecnologías.	Fallos en sistemas críticos que afecten las operaciones y generen pérdidas económicas.

CAPITULO II – ESTADO DEL ARTE.

2.1 INTRODUCCIÓN A COBIT 5.0.

COBIT 5.0 es un marco de referencia el cual fue desarrollado por ISACA para la gobernanza y la gestión de TI (tecnologías de la información) en las empresas. Proporciona un conjunto de guías y mejores prácticas para asegurar que la TI esté alineada con los objetivos estratégicos del negocio. Este marco ayuda a las empresas a crear un valor optimo desde TI, pudiendo así mantener un equilibrio entre la optimización de niveles de riesgos, el uso de los recursos y los beneficios.

Si hablamos de los beneficios que se obtienen al aplicar COBIT 5.0 podrías mencionar los siguientes:

Mejoras en la toma de decisiones: al aplicar esta metodología se obtiene información de alta calidad para poder apoyar las decisiones tomadas por las empresas.

Cumplimiento de regulaciones: la implementación de la metodología ayuda con el cumplimiento de normativas y regulaciones, reduciendo de esa forma los riegos legales.

Optimización de costos: facilita la gestión de los recursos de TI, ayudando así a la reducción de costos innecesarios.

Alineación estratégica: Asegura que las TI estén alineadas con los objetivos estratégicos de la organización.

Seguridad de la información: Mejora la gestión de riesgos y la seguridad de la información.

Logros al Aplicar COBIT 5.0

1. Mejora en la Calidad de los Servicios de TI:

Con la integración de esta metodología se asegura que los servicios de TI sean de alta calidad y cumplan con las expectativas de los usuarios

2. Gestión de la Continuidad del Negocio:

Ayuda a desarrollar y mantener planes de continuidad del negocio efectivos.

3. Fortalecimiento de la seguridad de la información:

Protección de los datos y sistemas de la organización contra amenazas externas e internas.

4. Aumento de la competitividad:

Aprovechamiento de las tecnologías de la información para obtener una ventaja competitiva.

La implementación exitosa de COBIT 5.0 requiere un compromiso a largo plazo por parte de la alta dirección y de todas las áreas de la organización. Los beneficios de esta adopción se manifiestan en una mejora continua de la gestión de TI, una mayor confianza de las partes interesadas y una mayor capacidad para adaptarse a los cambios del entorno empresarial.

2.2 PROPOSITO DE COBIT 5.0.

El propósito principal de COBIT 5.0 es proporcionar un marco estructurado que incluye objetivos de control, procesos y políticas, permitiendo a las organizaciones alinear sus iniciativas de TI con los objetivos estratégicos del negocio. Este marco ofrece una visión integral de la gestión de TI, abarcando desde la planificación estratégica hasta la operación diaria de los sistemas.

COBIT 5.0 facilita la evaluación, el seguimiento y la mejora continua de los procesos de TI, asegurando que se cumplan los requisitos de calidad, seguridad y cumplimiento normativo. Al adoptar COBIT 5.0, las organizaciones pueden maximizar el valor de sus inversiones en TI, mitigar riesgos y mejorar su competitividad en un entorno empresarial cada vez más digitalizado.

2.3 PRINCIPIOS DE COBIT 5.0.

Los principios de la metodología COBIT 5.0 son los siguientes:

1. Satisfacer las necesidades de las partes interesadas.

Con este principio se pretenden alinear las necesidades y las expectativas de las partes interesadas con los objetivos que tiene la organización. Se busca realizar una optimización al uso de los recursos para obtener beneficios con niveles de riesgos aceptables.

2. Cubrir la organización de forma integral.

Mediate este principio se busca tener una visión global de la organización, asegurando así que el gobierno y la gestión de TI estén cubriendo todas las áreas y procesos relevantes que se llevan a cabo en la empresa. Esto significa que no solo se enfoca en los aspectos técnicos, sino también en cómo la TI se integra y apoya todos los niveles y funciones de la empresa, desde la estrategia hasta las operaciones diarias.

3. Aplicar un solo marco integrado.

Mediante este principio se promueve el uso de un marco de referencia único que integre las mejores prácticas y estándares internacionales. COBIT 5.0 se alinea con otros marcos y estándares como ITIL, ISO, y TOGAF, proporcionando una estructura coherente y unificada para el gobierno y la gestión de TI.

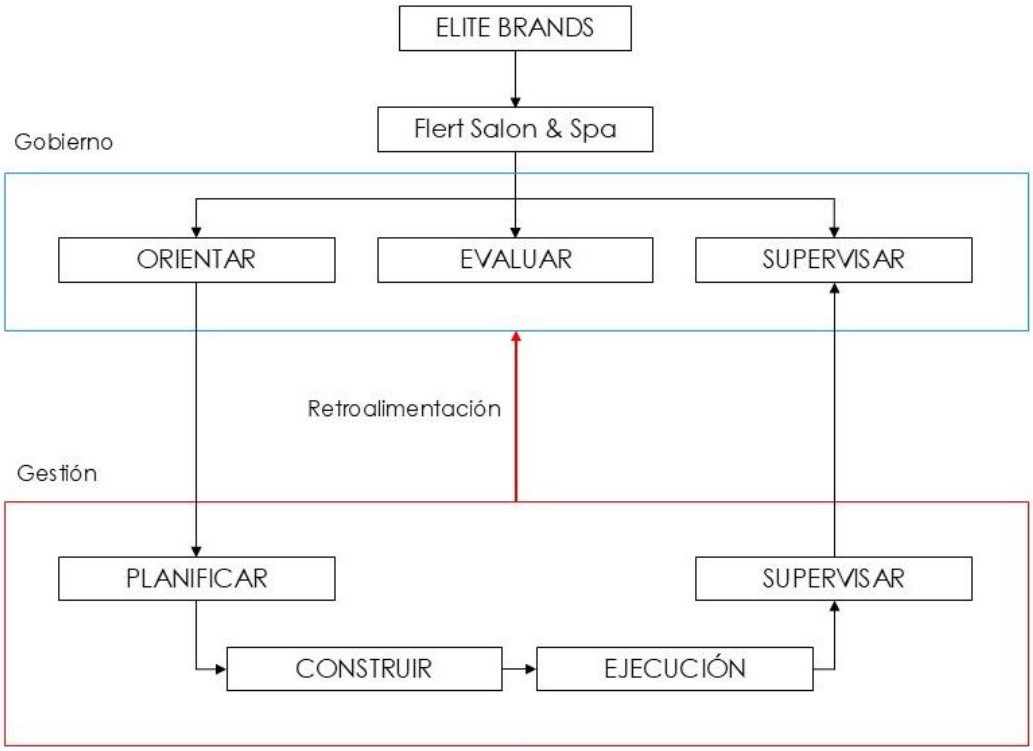
4. Habilitar un enfoque holístico.

Los habilitadores de COBIT 5 están identificados en siete categorías que abarcan la empresa de punta a punta. Individual y colectivamente, estos factores influyen para que el gobierno de TI y la gestión de TI operen en función de las necesidades del negocio.

5. Separar el gobierno de la administración.

Este principio establece una clara división de poderes entre el gobierno y la gestión de TI. Mientras el gobierno se encarga de definir la estrategia, establecer políticas y supervisar el cumplimiento, la gestión se centra en la ejecución diaria de las operaciones. Esta separación garantiza una gobernanza efectiva y una gestión eficiente de los recursos tecnológicos.

2.4 MODELO DE GOBIERNO DE COBIT 5.0.



Gobierno

ORIENTAR: Esta fase se enfoca en establecer la dirección estratégica y las políticas para la organización. Aquí se definen los objetivos y se alinean con las necesidades del negocio.

EVALUAR: En esta fase, se revisan y evalúan los resultados y el desempeño en relación con los objetivos establecidos. Se identifican áreas de mejora y se aseguran de que las políticas y estrategias estén siendo efectivas.

SUPERVISAR: Esta fase implica la supervisión continua de los procesos y actividades para asegurar que se cumplan los objetivos y se mantenga la conformidad con las políticas y regulaciones.

Gestión

PLANIFICAR: En esta fase, se desarrollan planes detallados para implementar las estrategias y políticas definidas en la fase de orientación. Incluye la asignación de recursos y la definición de cronogramas.

CONSTRUIR: Aquí se lleva a cabo la construcción y desarrollo de las soluciones y procesos necesarios para cumplir con los planes establecidos. Incluye el diseño, desarrollo y prueba de sistemas y procesos.

EJECUCIÓN: Esta fase se centra en la implementación y operación de las soluciones y procesos desarrollados. Se asegura de que todo funcione según lo planeado y se realizan ajustes según sea necesario.

SUPERVISAR: Similar a la fase de gobierno, esta fase en gestión también implica la supervisión continua para asegurar que los procesos se ejecuten correctamente y se logren los objetivos.

Retroalimentación: Es el proceso de recibir y analizar la información de retorno para realizar mejoras continuas en el sistema. Esta retroalimentación es crucial para ajustar y optimizar tanto las fases de gobierno como de gestión.

2.5 NIVELES DE MADUREZ DE COBIT 5.0.

El modelo de madurez para la administración y el control de procesos de TI se basa en un método de evaluación de la organización, de tal forman que

se pueda evaluar así misma desde un nivel de no-existe (0) hasta un nivel de optimizado.

• Nivel 0: En esta etapa los procesos no llegan a cumplir los propósitos o cubrir las necesidades, por lo cual este nivel se cataloga como incompleto.

• Nivel 1: En esta etapa los procesos cumplen sus propósitos, este nivel se cataloga como ejecución.

• Nivel 2: En esta etapa los procesos cumplen sus propósitos y consigo son gestionados para elevar la eficiencia y se lleve un control para su ejecución, este nivel se cataloga como gestionado.

• Nivel 3: En esta etapa el proceso alcanza estándares en donde es capaz el proceso en si dar resultados, este nivel se cataloga como establecido.

• Nivel 4: En esta etapa los procesos ya son bastantes controlados y son capaz de medirse para poder saber en cuanto tiempo son ejecutados y con este poder mejorar los tiempos, este nivel se cataloga como predecible.

• Nivel 5: En esta etapa los procesos ya se conocen como son ejecutados, se manejan los tiempos y estos son mejorados constantemente, para cumplir con exactitud las metas, este nivel se cataloga como optimizado.

2.6 IMPORTANCIA DEL MANEJO DE TI EN LAS EMPRESAS.

El manejo de TI es importante para la seguridad de los datos empresariales. Implementar sistemas de seguridad como firewalls, encriptación y detección de intrusos protege la información sensible contra ciberataques y accesos no autorizados, asegurando la confidencialidad e integridad de los datos.

Además, TI facilita el cumplimiento de normativas legales y regulaciones sobre protección de datos ya que las empresas pueden implementar políticas y procedimientos adecuados para garantizar que manejan los datos de manera responsable y conforme a la ley.

También tener un área de TI mejora la eficiencia operativa y la toma de decisiones. Automatizar procesos y analizar datos permite a las empresas optimizar sus operaciones, identificar oportunidades de mejora y tomar decisiones informadas, lo que contribuye a su competitividad y sostenibilidad en el mercado.

CAPITULO III. AUDITORÍA DEL AREA DE INFORMATICA UTILIZANDO LA METODOLOGIA DE COBÍT 5.0

3.1 DEFINIR EL OBJETIVO DE LA AUDITORÍA A DESARROLLAR.

Objetivo General:

- Optimizar la gobernanza y gestión de las tecnologías de la información en Flert Salon & Spa mediante la aplicación de la metodología COBIT 5.0, con el fin de alinear las prácticas del departamento de TI con los objetivos estratégicos de la empresa.

Objetivos Específicos sobre la auditoria para FLERT SALON & SPA:

- Asegurar que todas las decisiones de TI estén alineadas con las expectativas y necesidades de las partes interesadas, maximizando el valor generado por la tecnología y la información.
- Integrar la gobernanza y gestión de TI en todos los niveles de la organización, asegurando que todos los procesos y funciones de TI estén alineados con los objetivos estratégicos de la empresa.
- Implementar un marco de gobernanza de TI que combine y alinee las mejores prácticas y estándares internacionales, facilitando una gestión coherente y eficiente de los recursos de TI.
- Adoptar una perspectiva integral en la gestión de TI que considere todos los factores interrelacionados, optimizando el uso de recursos y minimizando riesgos a través de una visión completa del entorno de TI.

- Diferenciar claramente entre las funciones de gobierno, que se centran en la toma de decisiones estratégicas y la creación de políticas, y las funciones de gestión, responsables de la ejecución operativa.

3.2 DEFINIR EL ALCANCE DE LA AUDITORÍA DESARROLLAR.

- Identificar áreas de mejora en la gestión de TI de FLERT SALON & SPA, alineadas con los objetivos empresariales.
- Analizar los procesos actuales de TI en FLERT SALON & SPA utilizando COBIT 5.0 para medir su efectividad y cumplimiento normativo.
- Proponer acciones correctivas para los procesos que no estén bajo control adecuado en FLERT SALON & SPA.
- Desarrollar una mejora específica para un proceso con bajo rendimiento en la evaluación de FLERT SALON & SPA.

3.3 DEFINIR LA METODOLOGÍA DE TRABAJO.

Metodología de trabajo Grupal.

La metodología de trabajo que desarrollaremos está basada en 2 reuniones semanales de 2 a 3 horas aproximadamente ya sea de forma presencial o por videoconferencias. Donde se abordarán las actividades correspondientes a cada semana, en estas se asignará el trabajo que le corresponde a cada uno de los colaboradores. En la segunda reunión revisar el trabajo que se ha realizado y si se necesita mejorar será comunicado por parte del líder para que se hagan los cambios pertinentes antes de realizar entregar.

Metodología Basada en COBIT 5.0

1. Satisfacer las necesidades de las partes interesadas.

El principio de satisfacer las necesidades de las partes interesadas se centra en identificar y equilibrar las expectativas de todos los involucrados en el proceso de auditoría. En Flert Salon & Spa, esto implica trabajar estrechamente con los directivos, empleados y clientes para comprender sus objetivos en relación con el área de TI. COBIT 5.0 ayuda a garantizar que las decisiones y mejoras en TI agreguen valor a la organización al alinearse con las metas estratégicas, tales como el crecimiento del negocio, la satisfacción del cliente y la eficiencia operativa. Se implementan indicadores y métricas clave que permiten medir cómo las soluciones de TI contribuyen al logro de esos objetivos.

2. Cubrir la organización de forma integral.

COBIT 5.0 asegura una cobertura integral de toda la organización al no limitarse a auditar el departamento de TI de manera aislada. La metodología toma en cuenta cómo las tecnologías de la información impactan en todas las áreas de Flert Salon & Spa, desde la gestión administrativa hasta la experiencia del cliente. Esto significa que se auditan procesos, sistemas, infraestructuras y su interacción con las operaciones del negocio, asegurando que la gestión de TI esté alineada con todos los niveles de la empresa y sus diferentes funciones. Esta visión holística es clave para detectar posibles riesgos, oportunidades de mejora y asegurar la eficiencia global.

3. Aplicar un solo marco integrado.

El marco COBIT 5.0 se utiliza como la base unificadora para gestionar y gobernar los recursos de TI en Flert Salon & Spa. Este principio permite integrar otras normas y mejores prácticas ya existentes, como ISO 27001 para la seguridad de la información o ITIL para la gestión de servicios de TI. La metodología de trabajo busca consolidar estos marcos dentro de COBIT 5.0,

permitiendo una gestión eficiente y coherente. Esto asegura que el área de TI no esté implementando múltiples metodologías de manera aislada, sino que todas se integren en un solo enfoque estructurado y alineado con los objetivos estratégicos de la organización.

4. Habilitar un enfoque holístico

COBIT 5.0 utiliza un enfoque holístico al considerar múltiples factores que influyen en el éxito de la gestión de TI. En Flert Salon & Spa, esto implica tener en cuenta no solo los procesos tecnológicos, sino también los recursos, las personas, la cultura organizacional y la estructura de gobernanza. Cada uno de estos componentes actúa como un "habilitador" del éxito de TI, y la metodología de trabajo asegura que todos se optimicen de manera conjunta. Esto permite una evaluación completa, donde se identifican las fortalezas y debilidades no solo del sistema tecnológico, sino también del entorno organizacional que lo soporta.

5. Separar el gobierno de la administración

Este principio clave de COBIT 5.0 establece una distinción clara entre las actividades de gobernanza y administración. La gobernanza se refiere a las decisiones estratégicas que aseguran que TI esté alineada con los objetivos de negocio de Flert Salon & Spa, mientras que la administración abarca la implementación operativa de esas decisiones. En la metodología de trabajo, este principio se refleja en la creación de roles y responsabilidades definidos, donde la alta dirección supervisa y toma decisiones estratégicas, mientras que el personal de TI se encarga de la ejecución y operación diaria. Este enfoque asegura que las acciones cotidianas estén en sintonía con la visión y las metas a largo plazo de la organización.

3.4 DEFINIR LOS RECURSOS REQUERIDOS: PERSONAL, FINANCIERO Y HERRAMIENTAS.

Recurso Humano.

Nombre	Cargo	Habilidades Blandas	Habilidades Técnicas	Fortalezas	Debilidades
Javier Mejía	Líder	Responsabilidad, adaptabilidad y comunicación.	bases de datos, desarrollo de software y redes.	Orientación a resultados, proactividad y relaciones interpersonales.	La investigación.
Fátima Ayala	Auditores	Empatía y trabajo en equipo, adaptabilidad y comunicación y Manejo de conflictos.	Experiencia y resolución de problemas.	Trabajo en equipo y manejo de presión.	Dificultad para decir "no" y procrastinación e inseguridad en nuevas responsabilidades.
Fernando Chevez	Auditores	Comunicación efectiva y ayuda en la resolución de conflictos	Rápida adaptación a nuevas tecnologías	Capacidad de colaboración y trabajo en equipo.	Baja eficiencia en la priorización de tareas diarias.

Materiales:

Descripción	Costo Mensual	Meses	Costo
Transporte	$25.00	5	$ 125.00
Comida	$120.00	5	$ 600.00
Internet	$57.00	5	$ 285.00
Total			$ 1,010.00

Recursos Financieros:

Nombre	Cargo	Salario Mensual	Meses	Costo
Javier Mejía	Líder	$ 1,800.00	5	$ 9,000.00
Fátima Ayala	Colaboradores	$ 1,700.00	5	$ 7,500.00
Fernando Chévez	Colaboradores	$ 1,700.00	5	$ 7,500.00
Total				$ 24,000.00

Costo Total:

Descripción	Costo
Materiales	$ 1,010.00
Recursos Financieros	$ 24,000.00
Total	$ 25,010.00

3.5 DEFINIR EL TIEMPO REQUERIDO PARA SU IMPLEMENTACIÓN.

	Descripción	Tiempo
Semana 1	Análisis de conceptos de auditoria en informática, diferencia entre auditoria y consultoría.	15 de julio al 21 de julio de 2024
Semana 2	Entrevista sobre tipos de auditoría.	22 de julio al 28 de julio de 2024
Semana 3	Aplicando auditoria de programas a computadoras personales.	29 de julio al 11 de agosto de 2024 (Incluyendo vacaciones de agosto)
Semana 4	Reconocimiento de la empresa y aplicando COBIT 5.0.	12 de agosto al 18 de agosto de 2024
Semana 5	Conociendo las leyes en materia de informática existentes en el país.	19 de agosto al 25 de agosto de 2024
Semana 6	Defensa sobre la presentación de la empresa.	26 de agosto al 1 de septiembre de 2024
Semana 7	Comparación de COBIT 5.0 con otros marcos de trabajo	2 de septiembre al 8 de septiembre de 2024
Semana 8	Identificación de las necesidades de la empresa a auditar	9 de septiembre al 15 de septiembre de 2024
Semana 9	Formulación de preguntas adaptadas a la escala de Likert y tabulación de datos de respuestas de las partes interesadas.	16 de septiembre al 22 de septiembre de 2024.
Semana 10	Tabulación de datos para la obtención de	23 de septiembre al 29 de septiembre.

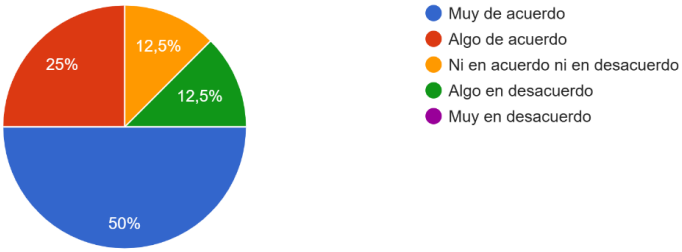
	datos de Metas de TI de la empresa.	
Semana 11	Evaluación de las metas de TI con las métricas de los procesos habilitantes, para obtener los procesos con deficiencia en la empresa.	30 de septiembre al 6 de octubre de 2024.
Semana 12	Evaluación de procesos relacionados a la unidad de TI.	7 de octubre al 13 de octubre de 2024.
Semana 13	Defensa de Mapeo de metas de la empresa	14 de octubre al 20 de octubre de 2024.
Semana 14	Evaluación técnica de los procesos habilitantes.	21 de octubre al 27 de octubre de 2024.
Semana 15	Descripción de los procesos con menor puntuación y matriz RACI.	28 de octubre al 3 de noviembre de 2024.
Semana 16	Definir las entradas y salidas, actividades de los procesos.	4 de noviembre al 10 de noviembre de 2024.
Semana 17	Definición de los posibles riesgos que se presentan en cada uno de los procesos, en la matriz de riesgos	11 de noviembre al 17 de noviembre de 2024.
Semana 18	Propuesta de políticas a implementar	18 de noviembre al 24 de noviembre de 2024.
Semana 19	Planteamiento de Beneficios y costos de la implementación de las políticas.	25 de noviembre al 1 de diciembre de 2024.
Semana 20	Defensa de reporte final de auditoría.	2 de diciembre al 8 de diciembre de 2024.

3.6 IDENTIFICANDO LAS NECESIDADES DE LAS PARTES INTERESADAS DE LA EMPRESA FLERT SALON & SPA.

Gráficas correspondientes al formulario proporcionado a los empleados de la empresa Flert Salon & Spa.

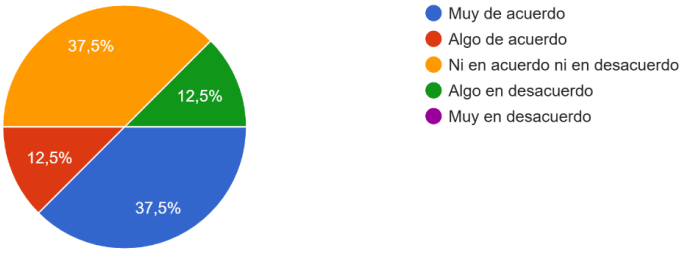
5. Creo que dependo de proveedores externos de TI en un nivel adecuado, y también que los acuerdos de externalización de TI están bien gesti...emás que se están verificando estos proveedores.

8 respuestas



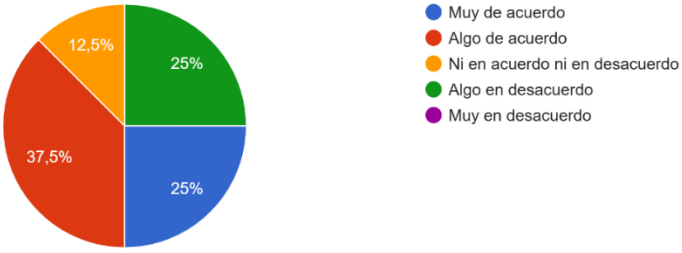
10. Identifico que el personal de TI es suficiente, y de qué manera puedo desarrollar y mantener sus habilidades mientras gestiono adecuadamente su rendimiento.

8 respuestas



13. Identifico que la capacidad de respuesta puede mejorar mediante la creación de un entorno de TI más flexible.

8 respuestas



3.6.1 ¿CÓMO HACER EL ANÁLISIS DE LAS NECESIDADES DE LAS PARTES INTERESADAS?

Para la evaluación de las respuestas en este estudio, se empleará la escala de Likert como método de medición. Esta escala es ampliamente utilizada para captar la opinión, actitud o nivel de acuerdo de los participantes ante una serie de afirmaciones. Consta de cinco niveles que van desde "Muy de acuerdo" hasta "Muy en desacuerdo", permitiendo que los encuestados seleccionen la opción que mejor refleje su postura frente a las declaraciones presentadas.

Se presenta la siguiente tabla de relación del criterio con su calificación pertinente basado en la escala de Likert:

CRITERIO	CALIFICACIÓN
Muy de acuerdo	5
Algo de acuerdo	4
Ni de acuerdo ni en desacuerdo	3
Algo en desacuerdo	2
Muy en desacuerdo	1

3.7 RELACIONANDO LAS NECESIDADES DE LAS PARTES INTERESADAS DE EMPRESA FLERT SALON & SPA CON LAS METAS DE NEGOCIO

ANÁLISIS DE LAS PARTES INTERESADAS FLERT SALON & SPA																															
Nº	NECESIDADES DE LOS INTERESADOS INTERNOS	AREAS																													
		GERENCIA/PROPIETARIO						EMPLEADO TI						EMPLEADOS EN GENERAL						CLIENTES						PROVEEDORES						PROMEDIO GLOBAL
		1	2	3	4	5	PROMEDIO	1	2	3	4	5	PROMEDIO	1	2	3	4	5	PROMEDIO	1	2	3	4	5	PROMEDIO	1	2	3	4	5	PROMEDIO	
1	Identifico que una parte considerable del esfuerzo de TI se destina a resolver problemas urgentes, en lugar de facilitar mejoras estratégicas.				4		0.8		2	3			1			3	4		1.4			3	4		1.4				4		0.8	1.08
2	Identifico que la capacidad de respuesta puede mejorar mediante la creación de un entorno de TI más flexible.					5	1		2		4		1.2		2		4		1.2			3	4		1.4					5	1	1.16
3	Pienso que los recursos y la infraestructura de TI disponibles son suficientes para alcanzar los objetivos estratégicos requeridos.				4		0.8					10	2			3	4		1.4			3	4		1.4				4		0.8	1.28
4	Identifico que el personal de TI es suficiente, y de qué manera puedo desarrollar y mantener sus habilidades mientras gestiono adecuadamente su rendimiento.					5	1			3	4		1.4			3	4		1.4			3		5	1.6					5	1	1.28
5	Opino que el tiempo que se toma en la toma de decisiones importantes sobre TI es adecuado para no afectar el desarrollo.					5	1			3	4		1.4				4	5	1.8			6			1.2					5	1	1.28
6	Creo que dependo de proveedores externos de TI en un nivel adecuado, y también que los acuerdos de externalización de TI están bien gestionados, además que se están verificando estos proveedores.					5	1				4	5	1.8				4	5	1.8		2	3			1					5	1	1.32
7	Considero que el costo de TI está controlado eficientemente, que los recursos se usan de la forma más eficaz posible y existen mejores opciones de aprovisionamiento.					5	1				4	5	1.8			3	4		1.4			3	4		1.4					5	1	1.32
8	Siento que el esfuerzo y las inversiones totales en TI son transparentes y están claramente comunicados a todas las partes interesadas.					5	1					10	2				8		1.6			6			1.2					5	1	1.36
9	Creo que se aprovechan adecuadamente la tecnología de red para generar nuevas oportunidades estratégicas.					5	1				4	5	1.8				8		1.6			3	4		1.4					5	1	1.36
10	Creo que se han contemplado todos los riesgos relacionados con TI.					5	1				4	5	1.8				8		1.6			3	4		1.4					5	1	1.36
11	Considero que el rendimiento de TI está bien gestionado.					5	1				4	5	1.8				4	5	1.8			3	4		1.4					5	1	1.40
12	Estoy satisfecho con la estructura y organización del departamento de TI.					5	1				4	5	1.8					10	2			6			1.2					5	1	1.40
13	Pienso que los requisitos de control para la información están claramente definidos.					5	1				4	5	1.8					10	2			6			1.2					5	1	1.40
14	Creo que los presupuestos de operación de TI no han excedido los límites de los proyectos y mantienen el presupuesto originalmente planeado.					5	1				4	5	1.8					10	2			6			1.2					5	1	1.40
15	Creo que las operaciones de TI respaldan el cumplimiento de la normativa y los niveles de servicio, y cómo puedo asegurarme de que todas las normas aplicables se cumplen correctamente.					5	1				4	5	1.8					10	2			6			1.2					5	1	1.40
16	Siento que estoy ejecutando una operación de TI eficiente y robusta.					5	1				4	5	1.8					10	2			3	4		1.4					5	1	1.44
17	Siento que puedo generar confianza en el funcionamiento y manejo de TI.					5	1					10	2					10	2			6			1.2					5	1	1.44
18	Opino que la información procesada está debidamente asegurada y protegida contra posibles riesgos.					5	1					10	2					10	2			6			1.2					5	1	1.44
19	Considero que los procesos críticos dependen de TI y que sus requerimientos están alineados con los objetivos.					5	1					10	2					10	2			6			1.2					5	1	1.44
20	Considero que los proyectos de TI cumplen con lo prometido y contribuyen al avance en la ejecución de la estrategia de negocio.					5	1				4	5	1.8					10	2			3		5	1.6					5	1	1.48
21	Percibo que se obtiene un valor significativo mediante el uso de TI y estoy satisfecho con la calidad del servicio de TI recibido.					5	1					10	2					10	2				4	5	1.8					5	1	1.56
22	Considero que las Tecnologías de Información son fundamentales para mantener un funcionamiento adecuado y eficiente.					5	1					10	2					10	2				4	5	1.8					5	1	1.56

3.8 OBTENIENDO LAS METAS DE TI PARA LA EMPRESA FLERT SALON & SPA.

NECESIDADES DE LAS PARTES INTERESADAS	METAS CORPORATIVAS DE COBIT 5.0																	
	1. Valor para las partes interesadas de las Inversiones de Negocio	2. Cartera de productos y servicios competitivos	3. Riesgos de negocio gestionados (salvaguarda de activos)	4. Cumplimiento de leyes y regulaciones externas	5. Transparencia financiera	6. Cultura de servicio orientada al cliente	7. Continuidad y disponibilidad del servicio de negocio	8. Respuestas ágiles a un entorno de negocio cambiante	9. Toma estratégica de Decisiones basada en Información	10. Optimización de costes de entrega del servicio	11. Optimización de la funcionalidad de los procesos de negocio	12. Optimización de los costes de los procesos de negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personas preparadas y motivadas	17. Cultura de innovación de producto y negocio	
	FINANCIERA					CLIENTE					INTERNA					APRENDIZAJE Y CRECIMIENTO		
Identifico que una parte considerable del esfuerzo de TI se destina a resolver problemas urgentes, en lugar de facilitar mejoras estratégicas.	1	1	5	1	0	5	5	1	0	1	1	1	0	5	1	5	0	33
Identifico que la capacidad de respuesta puede mejorar mediante la creación de un entorno de TI más flexible.	1	1	1	1	0	5	5	5	1	5	5	1	5	1	1	5	1	44
Pienso que los recursos y la infraestructura de TI disponibles son suficientes para alcanzar los objetivos estratégicos requeridos.	5	1	1	0	0	1	1	5	5	1	1	1	5	1	1	0	1	30
Identifico que el personal de TI es suficiente, y de qué manera puedo desarrollar y mantener sus habilidades mientras gestiono adecuadamente su rendimiento.	5	1	5	1	1	5	1	5	1	1	5	1	5	1	1	5	5	49
Opino que el tiempo que se toma en la toma de decisiones importantes sobre TI es adecuado para no afectar el desarrollo.	5	1	5	5	5	0	1	1	1	1	1	1	5	1	5	5	1	44
Creo que dependo de proveedores externos de TI en un nivel adecuado, y también que los acuerdos de externalización de TI están bien gestionados, además que se están verificando estos proveedores.	1	5	1	5	1	0	1	5	5	0	1	1	1	1	1	1	0	30
Considero que el costo de TI está controlado eficientemente, que los recursos se usan de la forma más eficaz posible y existen mejores opciones de aprovisionamiento.	5	1	1	1	5	1	1	1	0	5	1	5	0	1	5	1	0	34
PUNTUACIÓN	23	11	19	14	12	17	15	23	13	14	15	11	21	11	15	22	8	

	METAS CORPORATIVAS DE EMPRESA FLERT SALON & SPA	METAS CORPORATIVAS DE COBIT 5.0																	
		1. Valor para las partes interesadas de las inversiones de Negocio	2. Cartera de productos y servicios competitivos	3. Riesgos de negocio gestionados (salvaguarda de activos)	4. Cumplimiento de leyes y regulaciones externas	5. Transparencia financiera	6. Cultura de servicio orientada al cliente	7. Continuidad y disponibilidad del servicio de negocio	8. Respuestas ágiles a un entorno de negocio cambiante	9. Toma estratégica de Decisiones basada en información	10. Optimización de costes de entrega del servicio	11. Optimización de la funcionalidad de los procesos de negocio	12. Optimización de los costes de los procesos de negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personas preparadas y motivadas	17. Cultura de innovación de producto y negocio	
	METAS DE TI	**FINANCIERA**					**CLIENTE**					**INTERNA**					**APRENDIZAJE Y CRECIMIENTO**		**PUNTUACIÓN**
FINANCIERA	1. Alineamiento de TI y la estrategia de negocio.	5		1					1					5			1		13
	2. Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.	1		5					0					1			5		12
	3. Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI.	1		1					5					5			5		17
	4. Riesgos de negocio relacionados con las TI gestionados.	5		5					1					5			1		17
	5. Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI.	5		1					0					5			1		12
	6.Transparencia de los costes, beneficios y riesgos de las TI.	5		1					1					5			5		17
CLIENTE	7. Entrega de servicios de TI de acuerdo a los requisitos del negocio.	5		1					5					1			1		13
	8. Uso adecuado de aplicaciones, información y soluciones tecnológica.	1		5					1					1			5		13
INTERNA	9. Agilidad de las TI	1		1					5					5			5		17
	10. Seguridad de la información, infraestructuras,de procesamiento y aplicaciones.	5		5					1					5			5		21
	11 Optimización de activos, recursos y capacidades de las TI.	5		5					0					1			5		16
	12. Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnologia en procesos de negocio.	1		1					0					5			1		8
	13. Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	5		0					5					5			5		20
	14. Disponibilidad de información útil y relevante para la toma de decisiones.	1		0					5					5			1		12
	15. Cumplimiento de TI con las politicas internas.	1		5					1					1			1		9
APRENDIZAJE Y CONOCIMIENTO	16. Personal del negocio y de las TI competente y motivado.	1		1					5					5			5		17
	17. Conocimiento, experiencia e iniciativas para la innovación del negocio.	1		0					5					5			5		16
	PUNTUACIÓN	49	0	38	0	0	0	0	41	0	0	0	0	65	0	0	57	0	

Metas de TI encontradas.

METAS DE TI ENCONTRADAS
3. Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI.
4. Riesgos de negocio relacionados con las TI gestionados.
6.Transparencia de los costes, beneficios y riesgos de las TI.
9. Agilidad de las TI
10. Seguridad de la información, infraestructuras,de procesamiento y aplicaciones.
13. Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
16. Personal del negocio y de las TI competente y motivado.

			METAS DE TI FLERT SALON & SPA									
		0	3. Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI.	4. Riesgos de negocio relacionados con las TI gestionados.	6. Transparencia de los costes, beneficios y riesgos de las TI.		9. Agilidad de las TI	10. Seguridad de la información, infraestructuras,de procesamiento y aplicaciones.	13. Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.		16. Personal del negocio y de las TI competente y motivado.	
	ID	PROCESOS HABILITANTES DE COBIT 5.0	FINANCIERA			CLIENTE	INTERNA				APRENDIZAJE Y CRECIMIENTO	RESULTADO
EVALUAR, ORIENTAR Y SUPERVISAR	EDM01	Asegurar el establecimiento y mantenimiento del Marco de Gobierno	5									0.71
	EDM02	Asegurar la Entrega de Beneficios			1							0.14
	EDM03	Asegurar la Optimización de Riesgos		0	1			1				0.29
	EDM04	Asegurar la Optimización de los Recursos					1				0	0.14
	EDM05	Asegurar la transparencia hacia las partes interesadas	5		1							0.86
ALINEAR, PLANIFICAR Y ORGANIZAR	APO01	Gestionar el Marco de Gestión de TI					1				0	0.14
	APO02	Gestionar la Estrategia										0.00
	APO03	Gestionar la Arquitectura Empresarial					1					0.14
	APO04	Gestionar la Innovación					1					0.14
	APO05	Gestionar el Portafolio							5			0.71
	APO06	Gestionar el Presupuesto y los Costos			1							0.14
	APO07	Gestionar los Recursos Humanos							5		0	0.71
	APO08	Gestionar las Relaciones										0.00
	APO09	Gestionar los Acuerdos de Servicio										0.00
	APO10	Gestionar los Proveedores		0			1					0.14
	APO11	Gestionar la Calidad							5			0.71
	APO12	Gestionar el Riesgo		0	1			1	5			1.00
	APO13	Gestionar la seguridad		0	1			1				0.29
CONSTRUCCIÓN ADQUISICIÓN E IMPLEMENTACIÓN	BAI01	Gestionar los Programas y Proyectos		0					5			0.71
	BAI02	Gestionar la Definición de Requisitos										0.00
	BAI03	Gestionar la Identificación y la Construcción de Soluciones										0.00
	BAI04	Gestionar la Disponibilidad y la Capacidad										0.00
	BAI05	Gestionar la Introducción de Cambios Organizativos							5			0.71
	BAI06	Gestionar los Cambios		0				1				0.14
	BAI07	Gestionar la Aceptación del Cambio y de la Transición										0.00
	BAI08	Gestionar el Conocimiento					1					0.14
	BAI09	Gestionar los Activos			1							0.14
	BAI10	Gestionar la Configuración										0.00
ENTREGAR, DAR SEVICIO Y SOPORTE	DSS01	Gestionar las Operaciones		0								0.00
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio		0								0.00
	DSS03	Gestionar los Problemas		0								0.00
	DSS04	Gestionar la Continuidad		0								0.00
	DSS05	Gestionar los Servicios de Seguridad		0				1				0.14
	DSS06	Gestionar los Controles de los Procesos del Negocio		0								0.00
SUPERVISIÓN, EVALUACIÓN Y VERIFICACIÓN	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad		0								0.00
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno		0								0.00
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos		0								0.00
RESULTADO			10	0	7	0	6	5	30	0	0	

3.9 OBTENIENDO LOS PROCESOS HABILITANTES COMO RESULTADO DE CRUZARLOS CON LAS METAS DE TI.

3.9.1 MARCO TEÓRICO

El programa de evaluación de COBIT está diseñado para proporcionar a las empresas una metodología repetible, fiable y robusta para la evaluación de la capacidad de sus procesos de TI. Estas evaluaciones normalmente se utilizan como parte del programa de mejora de los procesos de una empresa y luego se pueden utilizar para informar a la alta dirección ejecutiva de la empresa sobre la capacidad actual de sus procesos de TI y de los objetivos de mejora que deben tenerse en cuenta, para poder atender los requerimientos del negocio.

En COBIT 5.0 un proceso se define como 'una colección de prácticas influidas por las políticas y procedimientos de empresa que toma entradas de una serie de recursos (incluyendo otros procesos), manipula las entradas y produce salidas (p. ej., productos, servicios)'.

El modelo de referencia de procesos de COBIT 5 subdivide los procesos dos principales áreas de actividad – gobierno y gestión – divididas en dominios de procesos.

Procesos de Gobierno (EDM): Aseguran el cumplimiento de objetivos empresariales, evalúa necesidades, condiciones y opciones de los interesados, dirige a través de la priorización y toma de decisiones, supervisa (monitorea) el desempeño y cumplimiento contra la dirección y los objetivos acordados.

Procesos de Gestión (APO, BAI, DSS, MEA): Planea, Construye, Opera y Supervisa (Monitor) las actividades fijadas y acordadas por el cuerpo de gobierno.

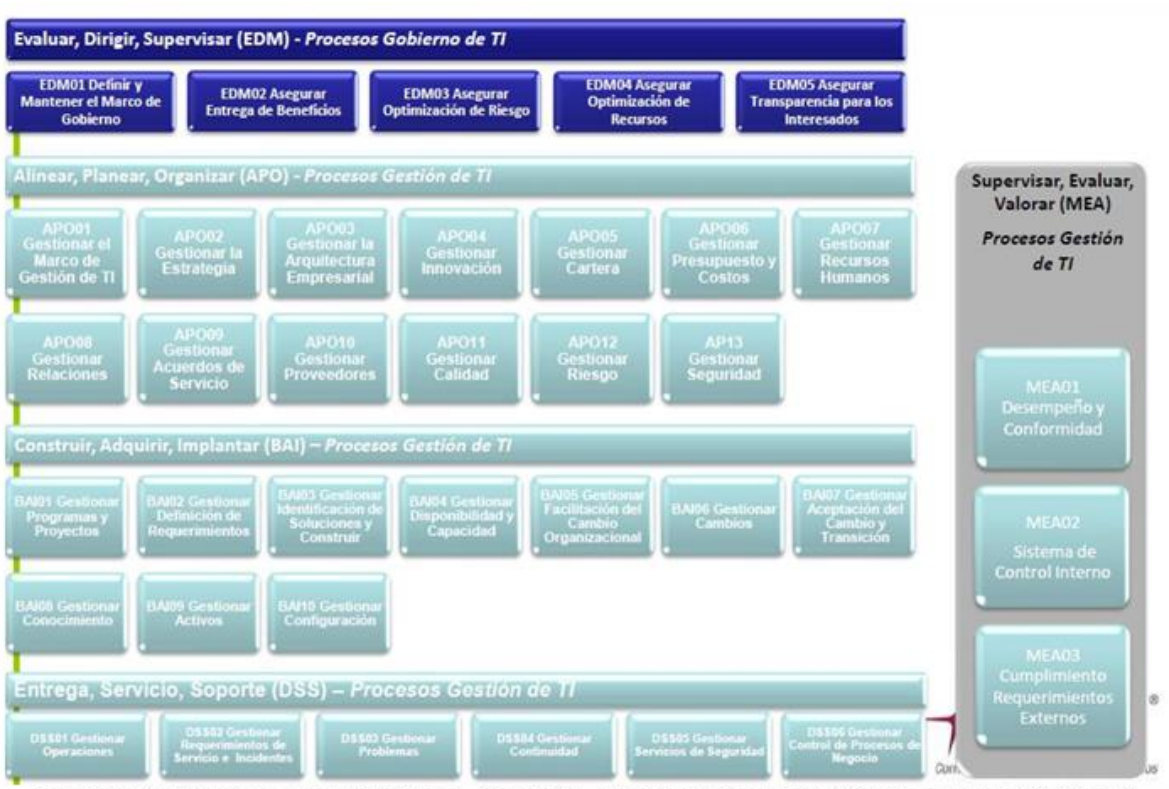


Imagen 1: Procesos de Gobierno - Gestión. Fuente: Procesos Catalizadores Cobit 5.0

TODOS LOS PROCESOS CONTIENEN.

Imagen 2: Estructura de un proceso. Fuente: Procesos Catalizadores Cobit 5.0

Imagen 4: Estructura de un proceso. Fuente: Procesos Catalizadores Cobit 5.0

CAPITULO IV – PROPUESTA DE IMPLEMENTACIÓN DE PROCESOS.

Presentamos la evaluación de los procesos dónde resultan 3 dentro del nivel 1, los cuáles son el EDM03 con 73.14%, APO12 con 71.43% y APO13 con 43.78%

RESULTADOS DE EVALUACIÓN DE PROCESOS

Procesos ID	Nombre del Proceso	Nivel evaluado	Nivel objetivo	Nivel 0	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
Los Procesos para el Gobierno y Gestión de TI									
Evaluar,Dirigir y Monitorear									
EDM03	Asegurar la optimización del riesgo.	0-1	1	F	73.14%				
Alinear,Planificar y Organizar									
APO03	Administrar la Arquitectura Empresarial	0	1	N					
APO04	Gestionar la Innovación	0	1	N					
APO12	Gestionar el Riesgo	0-1	1	F	71.43%				
APO13	Gestionar la Seguridad	0-1	1	F	46.78%				
Construir,Adquirir e Implementar									
BAI09	Gestionar los Activos	0	1	N					

Se detallan los procesos a implementar.

EDM03 (Fátima Ayala)	Asegurar la Optimización del Riesgo	Evaluar, Dirigir y Monitorear (EDM)

APO12 (Javier Mejía)	Gestionar el Riesgo	Alinear, Planificar y Organizar (APO)

APO13 (Fernando Chévez)	Gestionar la seguridad	Alinear, Planificar y Organizar (APO)

4.1 DESCRIPCIÓN DEL PROCESO

EMD03 ASEGURAR LA OPTIMIZACIÓN DEL RIESGO.

(Fátima Ayala)

Asegurar que el apetito y la tolerancia al riesgo en FLERT SALON & SPA son comprendidos, claramente definidos y comunicados entre las partes interesadas, garantizando que cualquier riesgo relacionado con el uso de las TI, que pudiera afectar el valor y la operación eficiente del salón, es identificado y gestionado adecuadamente.

APO12 GESTIONAR EL RIESGO.

(Javier Mejía)

Identificar, evaluar y reducir de manera continua los riesgos relacionados con TI en FLERT SALON & SPA, asegurando que estos se mantengan dentro de los niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.

APO13 GESTIONAR LA SEGURIDAD

(Fernando Chevez)

Definir, operar y supervisar un sistema para la gestión de la seguridad de la información en FLERT SALON & SPA.

4.2 DECLARACIÓN DEL PROPÓSITO DEL PROCESO

EDM03 ASEGURAR LA OPTIMIZACIÓN DEL RIESGO.

(Fátima Ayala)

Asegurar que los riesgos de TI en FLERT SALON & SPA se mantengan dentro del nivel aceptable, gestionando su impacto en el valor del salón y minimizando cualquier incumplimiento que afecte su operación y reputación.

APO12 GESTIONAR EL RIESGO.

(Javier Mejía)

Integrar la gestión de riesgos empresariales relacionados con TI en FLERT SALON & SPA con la gestión de riesgos empresariales general (ERM), equilibrando los costos y beneficios asociados a la administración de estos riesgos.

APO13 GESTIONAR LA SEGURIDAD

(Fernando Chevez)

Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información que ocurren en FLERT SALON & SPA dentro de los niveles de apetito de riesgo de la empresa.

4.3 OBJETIVO

EDM03 ASEGURAR LA OPTIMIZACIÓN DEL RIESGO.

(Fátima Ayala)

Gestionar los riesgos de TI en FLERT SALON & SPA dentro de los niveles aceptables, protegiendo su valor y asegurando un control efectivo para minimizar cualquier impacto negativo en su operación y reputación.

APO12 GESTIONAR EL RIESGO.

(Javier Mejía)

Garantizar que los riegos relacionados con TI en FLERT SALON & SPA se gestionen de manera integrada y continua, alineando su control con la estrategia general de riesgos empresariales, y optimizando los recursos para equilibrar costos y beneficios en beneficio de la empresa.

APO13 GESTIONAR LA SEGURIDAD

(Fernando Chevez)

Garantizar que los riegos de seguridad relacionados con TI en FLERT SALON & SPA estén definidos en un Sistema de Gestión de Seguridad de la Información, su forma de controlarlos, prevenirlos y evitarlos.

4.4 DEFINIR LOS INDICADORES

EDM03 ASEGURAR LA OPTIMIZACIÓN DEL RIESGO.

(Fátima Ayala)

Metas de TI relacionadas

04 Riesgos de negocio relacionados con las TI gestionados.

06 Transparencia de los costes, beneficios y riesgos de las TI.

10 Seguridad de la información, infraestructura de procesamiento y aplicaciones.

15 Cumplimiento de las políticas internas por parte de las TI.

Métricas

04

• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos.

• Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos.

• Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI.

• Frecuencia de actualización del perfil de riesgo.

06

• Porcentaje de inversión en casos de negocio con costes y beneficios esperados relativos a TI claramente definidos y aprobados.

• Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados.

• Encuesta de satisfacción a las partes interesadas clave relativa al nivel de transparencia, comprensión y precisión de la información financiera de TI.

10

• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública.

• Número de servicios de TI con los requisitos de seguridad pendientes.

• Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados.

• Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías.

Matriz RACI

Matriz RACI EDM03

Práctica clave de gobierno	DIRECTOR EJECUTIVO	GERENTE DE OPERACIONES	JEFE DE OPERACIONES	CENTRO DE DISTRIBUCIÓN	CONTABILIDAD	INFORMÁTICA	MANTENIMIENTO	AUDITORIA INTERNA	GERENCIA COMERCIAL	SUPERVISORA DE VENTAS/MERCADEO	DIRECTORA TÉCNICA	PUBLICIDAD	GERENCIA DE TIENDAS	ESTILISTAS	CAJERAS	ESTETICISTAS	BARBERO
EDM03.01 Evaluar la gestión de riesgos	R	C	C			R		C	I	I							
EDM03.02 Orientar la gestión de Riesgos	R	C	C	I		R		C	I	I	I						
EDM03.03 Supervisar de riesgos.	R	C	C	I		R		C	I	I	I						

APO12 GESTIONAR EL RIESGO

(Javier Mejía)

Metas de TI relacionadas:

02 Cumplimiento y soporte de las TI al cumplimiento del negocio de las leyes y regulaciones externas.

04 Riesgos de negocio relacionados con las TI gestionados.

06 Transparencia de los costes, beneficios y riesgo de las TI.

10 Seguridad de la información, infraestructura de procesamiento y aplicaciones.

10 Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.

Métricas:

04 Riesgos de negocio relacionados con las TI gestionados.

- Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos.
- Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos.
- Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI.
- Frecuencia de actualización del perfil de riesgo.

06 Transparencia de los costes, beneficios y riesgo de las TI.

- Porcentaje de inversión en casos de negocio con costes y beneficios esperados relativos a TI claramente definidos y aprobados.
- Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados.
- Encuesta de satisfacción a las partes interesadas clave relativa al nivel de transparencia, comprensión y precisión de la información financiera de TI.

10 Seguridad de la información, infraestructura de procesamiento y aplicaciones.

- Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública.
- Número de servicios de TI con los requisitos de seguridad pendientes.

- Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados.
- Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías.

13 Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.

- Número de programas/proyectos ejecutados en plazo y en presupuesto.
- Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto.
- Número de programas que necesitan ser revisados significativamente debido a defectos de calidad.
- Coste del mantenimiento de aplicaciones respecto al coste total de TI.

Matriz RACI:

Matriz RACI APO12																
Práctica clave de gobierno	DIRECTOR EJECUTIVO	GERENTE DE OPERACIONES	JEFE DE OPERACIONES	CENTRO DE DISTRIBUCIÓN	CONTABILIDAD	INFORMÁTICA	MANTENIMIENTO	AUDITORIA INTERNA	GERENCIA COMERCIAL	SUPERVISORA DE VENTAS/MERCADEO	DIRECTORA TÉCNICA	PUBLICIDAD	GERENCIA DE TIENDAS	ESTILISTAS	CAJERAS	ESTETICISTAS	BARBERO

APO12.01 Recopilar datos	I					A		C		R	R					
APO12.02 Analizar el riesgo	I					A		R		R	C					
APO12.03 Mantener un perfil de riesgo	I					R		R		R	C					
APO12.04 Expresar el riesgo	I					A		C		R	C					
APO12.05 Definir un portafolio de acciones para la gestión de riesgos	I					R		C		R	C					
APO12.06 Responder al riesgo	I					A		C		R	R					

APO13 GESTIONAR LA SEGURIDAD

(Fernando Chevez)

Metas de TI relacionadas:

Meta 2: Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas.

Meta 4: Riesgos de negocio relacionados con las TI gestionados.

Meta 6: Transparencia de los costes, beneficios y riesgo de las TI.

Meta 10: Seguridad de la información, infraestructura de procesamiento y aplicaciones.

Meta 14: Disponibilidad de información útil y relevante para la toma de decisiones.

Métricas:

- Número de roles de seguridad claves claramente definidos
- Número de incidentes relacionados con la seguridad
- Nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa.
- Número de soluciones de seguridad que se desvían del plan.
- Número de soluciones de seguridad que se desvían de la arquitectura de la empresa.
- Número de servicios con alineamiento confirmado al plan de seguridad
- Número de incidentes de seguridad causados por la no observancia del plan de seguridad
- Número de soluciones desarrolladas con alineamiento confirmado al plan de seguridad

Matriz RACI:

Matriz RACI APO13

Práctica clave de gobierno	DIRECTOR EJECUTIVO	GERENTE DE OPERACIONES	JEFE DE OPERACIONES	CENTRO DE DISTRIBUCIÓN	CONTABILIDAD	INFORMÁTICA	MANTENIMIENTO	AUDITORIA INTERNA	GERENCIA COMERCIAL	SUPERVISORA DE VENTAS/MERCADEO	DIRECTORA TÉCNICA	PUBLICIDAD	GERENCIA DE TIENDAS	ESTILISTAS	CAJERAS	ESTETICISTAS	BARBERO
APO13.01 Establecer y mantener un SGSI.	C	C	C			R		C	C				C		I		
APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	C	C	C			R		C	C				C		C		
APO13.03 Supervisar y revisar el SGSI.		I	I			R		C	C				C		R		

4.5 ENTRADAS Y SALIDAS DEL PROCESO

EDM03 ASEGURAR LA OPTIMIZACIÓN DEL RIESGO.

(Fátima Ayala)

EDM03.01 Evaluar la Gestión de Riesgos

ENTRADAS	
NÚMERO	**DESCRIPCIÓN**
APO12.01	Factores y Problemas de riesgos emergentes.
Fuera del Ámbito de COBIT	Principios de la gestión de riesgos de la empresa.

SALIDAS	
NÚMERO	**DESCRIPCIÓN**
APO12.03	Guías de Apetitos de riesgo
APO12.03	Niveles de tolerancia de riesgos aprobados.
APO12.01	Evaluación de las actividades de gestión de riesgos.

EDM03.02 Orientar la gestión de riesgos

ENTRADAS	
NÚMERO	**DESCRIPCIÓN**

APO12.03	Perfil de riesgo agregado incluyendo el estado de las acciones de gestión del riesgo.
Fuera del Ámbito de COBIT	Perfiles y planes de mitigación de la Gestión de Riesgo de la Empresa (ERM)

SALIDAS	
NÚMERO	**DESCRIPCIÓN**
APO12.01	Políticas de Gestión e riesgos
APO12.01	Objetivos claves a ser monitorizados por la gestión de riesgos
APO12.01	Proceso aprobado para la medición de la gestión de riesgos.

EDM03.03 Supervisar la gestión de riesgos

ENTRADAS	
NÚMERO	**DESCRIPCIÓN**
APO12.02	Resultados de análisis de riesgos.
APO12.04	Resultados de las evaluaciones de riesgos de terceras partes

SALIDAS	
NÚMERO	**DESCRIPCIÓN**
APO12.06	Acciones correctivas para tratas las desviaciones en la gestión del riesgo.
EDM05.01	Problemas de la gestión de riesgos para la Dirección

APO12 GESTIONAR EL RIESGO.

(Javier Mejía)

APO12.01 Recopilar Datos

ENTRADAS	
NÚMERO	**DESCRIPCIÓN**
EDM03.01	Evaluación de actividades de riesgos.
EMD03.02	Políticas de gestión de riesgos.
APO02.02	Brechas y riesgos relacionados con capacidades actuales.
APO02.05	Evaluación del riesgo
APO10.04	Riesgo de entrega de proveedores identificado
DSS02.07	Estado de incidentes e informe de tendencias

SALIDAS	
NÚMERO	**DESCRIPCIÓN**
Interno	Datos en el entorno de operación relacionados con el riesgo
Interno	Datos en eventos de riesgo y en factores contribuyentes
EDM03.01 APO01.03 APO02.02	Elementos y factores de riesgo emergentes

APO12.02 Analizar el Riesgo.

ENTRADAS	
NÚMERO	**DESCRIPCIÓN**
DSS04.02	Análisis de impacto en el negocio
DSS05.01	Evaluaciones de amenazas potenciales
Fuera del Ámbito de COBIT	Avisos de amenaza

SALIDAS	
NÚMERO	**DESCRIPCIÓN**
Interno	Alcance de los esfuerzos de análisis de riesgos
Interno	Escenarios de riesgo de TI

EDM03.03 APO01.03 APO02.02 BAI01.10	Resultados de análisis de riesgos

APO12.03 Mantener un Perfil de Riesgo

ENTRADAS	
NÚMERO	**DESCRIPCIÓN**
EDM03.01	Guía de apetito al riesgo
APO10.04	Riesgo de entrega de proveedores identificado
DSS05.01	Evaluaciones de amenazas potenciales

SALIDAS	
NÚMERO	**DESCRIPCIÓN**
Interno	Escenarios de riesgo documentados por la línea de negocio y función
EDM03.02 APO02.02	Perfil de riesgo agregado, incluyendo el estado de las acciones de gestión del riesgo

APO12.04 Expresar el Riesgo

ENTRADAS	
NÚMERO	**DESCRIPCIÓN**

SALIDAS	
NÚMERO	**DESCRIPCIÓN**
EDM03.03 EDM05.02 APO10.04 MEA02.08	Análisis de riesgos e informes del perfil de riesgos para las partes interesadas
EDM03.03 APO10.04 MEA02.01	Revisión de resultados de evaluaciones de riesgos de terceras partes
EDM03.03	Oportunidades para la aceptación de un riesgo mayor

APO12.05 Definir un portafolio de acciones para la gestión de riesgos

ENTRADAS	
NÚMERO	**DESCRIPCIÓN**

SALIDAS	
NÚMERO	**DESCRIPCIÓN**
APO02.02 APO13.02	Propuestas de proyecto para reducir el riesgo

APO12.06 Responder al riesgo

ENTRADAS	
NÚMERO	**DESCRIPCIÓN**
EDM03.03	Acciones correctoras para tratar las desviaciones de gestión de riesgos

SALIDAS	
NÚMERO	**DESCRIPCIÓN**
DSS02.05	Planes de respuesta para incidentes relacionados con el riesgo
APO01.04 APO08.04 DSS04.02	Comunicaciones del impacto del riesgo
DSS02.03 DSS03.01	Causas raíz relacionadas con el riesgo

DSS03.02 DSS04.02 MEA02.04 MEA02.07 MEA02.08	

APO13 GESTIONAR LA SEGURIDAD

(Fernando Chevez)

APO13.01 Establecer y mantener un SGSI

ENTRADAS	
NÚMERO	**DESCRIPCIÓN**
Fuera del Ámbito de COBIT	Enfoque de seguridad de la empresa

SALIDAS	
NÚMERO	**DESCRIPCIÓN**
Interno	Política de SGSI
APO01.02 DSS06.03	Declaración de alcance del SGSI

APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.

ENTRADAS	
NÚMERO	**DESCRIPCIÓN**
APO02.04	Diferencias y cambios necesarios para alcanzar la capacidad objetivo

APO03.02	Descripciones de dominios de partida y definición de arquitectura
APO12.0	Propuestas de proyectos para reducir el riesgo

SALIDAS	
NÚMERO	**DESCRIPCIÓN**
Todo EDM Todo APO Todo BAI Todo DSS Todo MEA	Plan de tratamiento de riesgos de seguridad de la información
APO02.05	Declaración de alcance del SGSI

APO13.03 Supervisar y revisar el SGSI.

ENTRADAS	
NÚMERO	**DESCRIPCIÓN**
DSS02.02	Incidentes clasificados y priorizados y requerimientos de servicios

SALIDAS	
NÚMERO	**DESCRIPCIÓN**
MEA02.01	Informes de auditoría del SGSI
Interno	Recomendaciones para mejorar el SGSI

4.6 ACTIVIDADES

EDM03 ASEGURAR LA OPTIMIZACIÓN DEL RIESGO.

(Fátima Ayala)

EDM03.1

1. Determinar el nivel de riesgos relacionados con las TI que la empresa está dispuesta a asumir para cumplir con sus objetivos (apetito de riesgo).

2. Evaluar y aprobar propuestas de umbrales de tolerancia al riesgo TI frente a los niveles de riesgo y oportunidad aceptables por la empresa.

3. Determinar el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos empresariales.

4. Evaluar proactivamente los factores de riesgo TI con anterioridad a las decisiones estratégicas de la empresa pendientes y asegurar que las decisiones de la empresa se toman conscientes de los riesgos.

5. Determinar si el uso de TI está sujeto a una valoración y evaluación de riesgos adecuada, según lo descrito en estándares nacionales e internacionales relevantes.

6. Evaluar las actividades de gestión de riesgos para garantizar su alineamiento con las capacidades de la empresa para las perdidas relacionadas con TI y la tolerancia de los líderes a los mismos.

Activos de Información			Activos Físicos	Activos Humanos
COD	Manejo de Información de TI	Software	Hardware	Personal

EDM01.01	Determinar el nivel de riesgos relacionados con las TI que la empresa está dispuesta a asumir para cumplir con sus objetivos (apetito de riesgo).	Acher (RSA)	Computadora	Jefe de Unidad de TI
	Evaluar y aprobar propuestas de umbrales de tolerancia al riesgo TI frente a los niveles de riesgo y oportunidad aceptables por la empresa.	Resolver	Computadora	Jefe de Unidad de TI
	Determinar el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos empresariales.	Power Bi, Tableau	Computadora, Servidor	Jefe de la Unidad de TI

	Evaluar proactivamente los factores de riesgo TI con anterioridad a las decisiones estratégicas de la empresa pendientes y asegurar que las decisiones de la empresa se toman conscientes de los riesgos.	RiskWatch	Computadora	Jefe de la Unidad de TI
	Determinar si el uso de TI está sujeto a una valoración y evaluación de riesgos adecuada, según lo descrito en estándares nacionales e internacionales relevantes.	ISO/IEC 27001	Computadora	Jefe de Unidad de TI, Encargado de Soporte Técnico

	Evaluar las actividades de gestión de riesgos para garantizar su alineamiento con las capacidades de la empresa para las perdidas relacionadas con TI y la tolerancia de los líderes a los mismos.	HighBond	Computadora	Jefe de Unidad de TI, Encargado de Soporte Técnico

EDM03.02

1. Promover una cultura consciente de los riesgos TI e impulsar a la empresa a una identificación proactiva de riesgos TI, oportunidades e impactos potenciales en el negocio.

2. Orientar la integración de las operaciones y la estrategia de riesgos de TI con las decisiones y operaciones empresariales estratégicas.

3. Orientar la elaboración de planes de comunicación de riesgos (cubriendo todos los niveles de la empresa), así como los planes de acción de riesgo.

4. Orientar la implantación de mecanismos apropiados para responder rápidamente a los riesgos cambiantes y notificar inmediatamente a los niveles adecuados de gestión, soportados principios de escalado acordados (qué informar, cuándo, dónde y cómo).

5. Orientar para que el riesgo, las oportunidades, los problemas y preocupaciones puedan ser identificadas y notificadas por cualquier

persona en cualquier momento. El riesgo debe ser gestionado de acuerdo con las políticas y procedimientos publicados y escalados a los decisores relevantes.

6. Identificar los objetivos e indicadores clave de los procesos de gobierno y gestión de riesgos a ser monitorizados y aprobar los enfoques, métodos, técnicas y procesos para capturar y notificar la información de medición.

Activos de Información			Activos Físicos	Activos Humanos
COD	Manejo de Información de TI	Software	Hardware	Personal
EDM03.02	Promover una cultura consciente de los riesgos TI e impulsar a la empresa a una identificación proactiva de riesgos TI, oportunidades e impactos potenciales en el negocio.	Resolver	Computadora.	Jefe de Unidad de TI
	Orientar la integración de las operaciones y la estrategia de riesgos de TI con las decisiones y operaciones empresariales estratégicas.	Power BI	Computadora, Servidor de datos	Jefe de Unidad de TI

	Orientar la elaboración de planes de comunicación de riesgos (cubriendo todos los niveles de la empresa), así como los planes de acción de riesgo.	Microsoft Teams,	Computadora	Jefe de Unidad de TI, Encargado de Soporte Técnico
	Orientar la implantación de mecanismos apropiados para responder rápidamente a los riesgos cambiantes y notificar inmediatamente a los niveles adecuados de gestión, soportados principios de escalado acordados (qué informar, cuándo, dónde y cómo).	PagerDuty,	Computadora	Encargado de Soporte Técnico

	Orientar para que el riesgo, las oportunidades, los problemas y preocupaciones puedan ser identificadas y notificadas por cualquier persona en cualquier momento. El riesgo debe ser gestionado de acuerdo con las políticas y procedimientos publicados y escalados a los decisores relevantes.	JIRA	Computadora, Teléfonos Corporativos	Encargado de Soporte Técnico.
	Identificar los objetivos e indicadores clave de los procesos de gobierno y gestión de riesgos a ser monitorizados y aprobar los enfoques, métodos, técnicas y procesos para capturar y notificar la información de medición.	Archer (RSA)	Computadora	Jefe de Unidad de TI

EDM03.03

1. Supervisar hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de apetito de riesgo.

2. Supervisar las metas y métricas clave de gestión de los procesos de gobierno y gestión del riesgo respecto a los objetivos, analizar las causas de las desviaciones e iniciar medidas correctivas para abordar las causas subyacentes.

3. Facilitar la revisión por las principales partes interesadas del progreso de la empresa hacia los objetivos identificados.

4. Informar cualquier problema de gestión de riesgos al Consejo o al Comité de Dirección.

Activos de Información			Activos Físicos	Activos Humanos
COD	Manejo de Información de TI	Software	Hardware	Personal
EDM03.03	Supervisar hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de apetito de riesgo.	Archer (RSA)	Computadora	Jefe de Unidad de TI
	Supervisar las metas y métricas clave de gestión de los procesos de gobierno y gestión del riesgo respecto a los objetivos, analizar las causas de las desviaciones e iniciar medidas correctivas para abordar las causas subyacentes.	Power BI	Computadora, Servidor de datos.	Jefe de Unidad de TI

	Facilitar la revisión por las principales partes interesadas del progreso de la empresa hacia los objetivos identificados.	Microsoft Teams, Zoom	Computadora, Pantallas para reuniones.	Jefe de Unidad de TI, Encargado de Soporte Técnico
	Informar cualquier problema de gestión de riesgos al Consejo o al Comité de Dirección.	JIRA, Microsoft PowerPoint	Computadora, Proyector en sala de reuniones	Jefe de Unidad de TI

APO12 GESTIONAR EL RIESGO

(Javier Mejía)

APO12.01 Recopilar datos.

1. Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con riesgo de TI, dando cabida a múltiples tipos de eventos, múltiples categorías de riesgo de TI y múltiples factores de riesgo.

2. Registrar datos relevantes sobre el entorno de operación interno y externo de la empresa que pudieran jugar un papel significativo en la gestión del riesgo de TI.

3. Medir y analizar los datos históricos de riesgo de TI y de pérdidas experimentadas tomados de datos y tendencias externas disponibles, empresas similares de la industria – basados en eventos registrados, bases de datos y acuerdos de la industria sobre divulgación de eventos comunes.

4. Registrar datos sobre eventos de riesgo que han causado o pueden causar impactos al beneficio/valor facilitado por TI, a la entrega de programas y proyectos de TI y/o a las operaciones y entrega de servicio de

TI. Capturar datos relevantes sobre asuntos relacionados, incidentes, problemas e investigaciones.

5. Para clases o eventos similares, organizar los datos recogidos y destacar factores contribuyentes. Determinar los factores contribuyentes comunes para eventos múltiples.

6. Determinar las condiciones específicas que existían o faltaban cuando ocurrieron los eventos de riesgo y la forma en la cual las condiciones afectaban la frecuencia del evento y la magnitud de la pérdida.

7. Ejecutar análisis periódicos de eventos y de factores de riesgo para identificar asuntos nuevos o emergentes relacionados con el riesgo y para obtener un entendimiento de los asociados factores de riesgo internos y externos.

Activos de Información			Activos Físicos	Activos Humanos
COD	Manejo de Información de TI	Software	Hardware	Personal

APO12.01	Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con riesgo de TI, dando cabida a múltiples tipos de eventos, múltiples categorías de riesgo de TI y múltiples factores de riesgo.	Excel ServiceNow	PC y servidor de base de datos.	Jefe de Unidad de TI, Encargado de soporte técnico
	Registrar datos relevantes sobre el entorno de operación interno y externo de la empresa que pudieran jugar un papel significativo en la gestión del riesgo de TI.	Excel ServiceNow	Computadora, servidor de base de datos	Jefe de Unidad de TI

	Medir y analizar los datos históricos de riesgo de TI y de pérdidas experimentadas tomados de datos y tendencias externas disponibles, empresas similares de la industria – basados en eventos registrados, bases de datos y acuerdos de la industria sobre divulgación de eventos comunes.	MetricStream PowrBI	Computadora, servidor de base de datos	Encargado de soporte técnico

	Registrar datos sobre eventos de riesgo que han causado o pueden causar impactos al beneficio/valor facilitado por TI, a la entrega de programas y proyectos de TI y/o a las operaciones y entrega de servicio de TI. Capturar datos relevantes sobre asuntos relacionados, incidentes, problemas e investigaciones.	Jira Excel	Computadora, servidor de base de datos	Jefe de Unidad de TI, Encargado de soporte técnico

	Para clases o eventos similares, organizar los datos recogidos y destacar factores contribuyentes. Determinar los factores contribuyentes comunes para eventos múltiples.	Splunk PowerBI Excel	Computadora, servidor de base de datos	Encargado de soporte técnico
	Determinar las condiciones específicas que existían o faltaban cuando ocurrieron los eventos de riesgo y la forma en la cual las condiciones afectaban la frecuencia del evento y la magnitud de la pérdida.	RiskWatch Tableau Excel	Computadora, servidor de base de datos	Jefe de Unidad de TI

	Ejecutar análisis periódicos de eventos y de factores de riesgo para identificar asuntos nuevos o emergentes relacionados con el riesgo y para obtener un entendimiento de los asociados factores de riesgo internos y externos.	RiskLens PowerBI Excel	Computadora, servidor de base de datos	Jefe de Unidad de TI, Encargado de soporte técnico

APO12.02 Analizar el riesgo.

1. Definir la amplitud y profundidad apropiadas para los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y la criticidad en el negocio de los activos. Establecer el alcance del análisis de riesgos después de llevar a cabo un análisis coste-beneficio.

2. Construir y actualizar regularmente escenarios de riesgo de TI, que incluyan escenarios compuestos en cascada y/o tipos de amenaza coincidentes y desarrollar expectativas para actividades de control específicas, capacidades para detectar y otras medidas de respuesta.

3. Estimar la frecuencia y magnitud de pérdida o ganancia asociada con escenarios de riesgo de TI. Tener en cuenta todos los factores de riesgo que

apliquen, evaluar controles operacionales conocidos y estimar niveles de riesgo residual.

4. Comparar el riesgo residual con la tolerancia al riesgo e identificar exposiciones que puedan requerir una respuesta al riesgo.

5. Analizar el coste-beneficio de las opciones de respuesta al riesgo potencial, tales como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/ capturar. Proponer la respuesta al riesgo óptima.

6. Especificar requerimientos de alto nivel para los proyectos o programas que implementarán las respuestas de riesgo seleccionadas. Identificar requerimientos y expectativas para los controles clave que son apropiados para las respuestas de mitigación de riesgos.

7. Validar los resultados de análisis de riesgos antes de usarlos para la toma de decisiones, confirmando que los análisis se alinean con requerimientos de empresa y verificando que las estimaciones fueron apropiadamente calibradas y examinadas ante una posible parcialidad.

Activos de Información			Activos Físicos	Activos Humanos
COD	Manejo de Información de TI	Software	Hardware	Personal

APO12.02	Definir la amplitud y profundidad apropiadas para los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y la criticidad en el negocio de los activos. Establecer el alcance del análisis de riesgos después de llevar a cabo un análisis coste-beneficio.	RiskWatch.	Computadora y Servidor de base de datos.	Jefe de Unidad de TI.

	Construir y actualizar regularmente escenarios de riesgo de TI, que incluyan escenarios compuestos en cascada y/o tipos de amenaza coincidentes y desarrollar expectativas para actividades de control específicas, capacidades para detectar y otras medidas de respuesta.	RiskLens.	Computadora, servidor de bases de datos.	Jefe de Unidad de TI, Encargado de soporte técnico.

	Estimar la frecuencia y magnitud de pérdida o ganancia asociada con escenarios de riesgo de TI. Tener en cuenta todos los factores de riesgo que apliquen, evaluar controles operacionales conocidos y estimar niveles de riesgo residual.	Excel Base de Datos.	Servidor de base de datos, PC e impresoras.	Jefe de Unidad de TI.
	Comparar el riesgo residual con la tolerancia al riesgo e identificar exposiciones que puedan requerir una respuesta al riesgo.	AuditBoard	PC y servidor de bases de datos.	Jefe de Unidad de TI

	Analizar el coste-beneficio de las opciones de respuesta al riesgo potencial, tales como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/capturar. Proponer la respuesta al riesgo óptima.	RiskWatch Excel	PC y servidor de bases de datos.	Jefe de Unidad de TI, Encargado de soporte técnico

	Especificar requerimientos de alto nivel para los proyectos o programas que implementarán las respuestas de riesgo seleccionadas. Identificar requerimientos y expectativas para los controles clave que son apropiados para las respuestas de mitigación de riesgos.	Jira Microsoft Project	PC y sistemas de respaldo.	Encargado de soporte técnico

	Validar los resultados de análisis de riesgos antes de usarlos para la toma de decisiones, confirmando que los análisis se alinean con requerimientos de empresa y verificando que las estimaciones fueron apropiadamente calibradas y examinadas ante una posible parcialidad.	Power BI	PC, proyector, impresora para informes.	Jefe de Unidad de TI

APO12.03 Mantener un perfil de riesgo.

1. Inventariar los procesos de negocio, incluyendo el personal de soporte, aplicaciones, infraestructura, instalaciones, registros manuales críticos, vendedores, proveedores y externalizados y documentar la dependencia de los procesos de gestión de servicio TI y de los recursos de infraestructuras TI.

2. Determinar y acordar qué servicios TI y recursos de infraestructuras de TI son esenciales para sostener la operación de procesos de negocio. Analizar dependencias e identificar eslabones débiles.

3. Agregar escenarios de riesgo actuales, por categoría, línea de negocio y área funcional.

4. De forma regular, capturar toda la información sobre el perfil de riesgo y consolidarla dentro de un perfil de riesgo agregado.

5. Sobre la base de todos los datos del perfil de riesgo, definir un conjunto de indicadores de riesgo que permitan la identificación rápida y la supervisión del riesgo actual y las tendencias de riesgo.

6. Capturar información sobre eventos de riesgos de TI que se han materializado, para su inclusión en el perfil de riesgo de TI de la empresa.

7. Capturar información sobre el estado del plan de acción del riesgo, para la inclusión en el perfil de riesgo de TI de la empresa.

Activos de Información			Activos Físicos	Activos Humanos
COD	Manejo de Información de TI	Software	Hardware	Personal

APO12. 03	Inventariar los procesos de negocio, incluyendo el personal de soporte, aplicaciones, infraestructura, instalaciones, registros manuales críticos, vendedores, proveedores y externalizados y documentar la dependencia de los procesos de gestión de servicio TI y de los recursos de infraestructuras TI.	Excel	PC y servidor de base de datos.	Jefe de Unidad de TI, Encargado de soporte técnico

	Determinar y acordar qué servicios TI y recursos de infraestructuras de TI son esenciales para sostener la operación de procesos de negocio. Analizar dependencias e identificar eslabones débiles.	Archer PowerBI ServiceNow	PC	Jefe de Unidad de TI.
	Agregar escenarios de riesgo actuales, por categoría, línea de negocio y área funcional.	RiskWatch Jira Excel	PC, servidor de almacenamiento en la red (NAS)	Encargado de soporte técnico
	De forma regular, capturar toda la información sobre el perfil de riesgo y consolidarla dentro de un perfil de riesgo agregado.	Tableu Excel MetricStream	PC, servidor de almacenamiento en la red (NAS)	Jefe de Unidad de TI, Encargado de soporte técnico

	Sobre la base de todos los datos del perfil de riesgo, definir un conjunto de indicadores de riesgo que permitan la identificación rápida y la supervisión del riesgo actual y las tendencias de riesgo.	PowerBI MetricStream Excel	PC, servidor de almacenamiento en la red (NAS), proyectores	Jefe de Unidad de TI
	Capturar información sobre eventos de riesgos de TI que se han materializado, para su inclusión en el perfil de riesgo de TI de la empresa.	Jira ServiceNow Excel	PC, sistema de respaldo de datos, impresora	Encargado de soporte técnico

	Capturar información sobre el estado del plan de acción del riesgo, para la inclusión en el perfil de riesgo de TI de la empresa.	Archer Excel	PC, servidor de almacenamiento en la red (NAS).	Jefe de Unidad de TI, Encargado de soporte técnico.

APO12.04 Expresar el riesgo.

1. Informar de los resultados del análisis de riesgos a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones de empresa. Cuando sea posible, incluir probabilidades y rangos de pérdida o ganancia junto con niveles de confianza que permitan a la dirección equilibrar el retorno del riesgo.

2. Proporcionar a los responsables de toma de decisiones un entendimiento de los escenarios peor y más probable, exposiciones de diligencia debida y consideraciones sobre la reputación, legales y regulatorias significativas.

3. Informar el perfil de riesgo actual a todas las partes interesadas, incluyendo la efectividad del proceso de gestión de riesgos, la efectividad de los controles, diferencias, inconsistencias, redundancias, estado de la remediación y sus impactos en el perfil de riesgo.

4. Revisar los resultados de evaluaciones objetivas de terceras partes, auditorías internas y revisiones del aseguramiento de la calidad y mapearlos con el perfil de riesgo. Revisar las diferencias y exposiciones identificadas para determinar la necesidad de análisis de riesgos adicionales.

5. De forma periódica, para áreas con un riesgo relativo y una paridad de capacidad del riesgo, identificar oportunidades relacionadas con TI que podrían permitir la aceptación de un mayor riesgo y un crecimiento y retorno mayores.

Activos de Información			Activos Físicos	Activos Humanos
COD	Manejo de Información de TI	Software	Hardware	Personal

APO12.04	Informar de los resultados del análisis de riesgos a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones de empresa. Cuando sea posible, incluir probabilidades y rangos de pérdida o ganancia junto con niveles de confianza que permitan a la dirección equilibrar el retorno del riesgo.	PowerBI Tableu Excel	PC, proyectores, pantallas de visualización	Jefe de Unidad de TI, Encargado de soporte técnico

	Proporcionar a los responsables de toma de decisiones un entendimiento de los escenarios peor y más probable, exposiciones de diligencia debida y consideraciones sobre la reputación, legales y regulatorias significativas.	RickWatch Word Archer	PC, sistemas de respaldo de información.	Jefe de Unidad de TI

	Informar el perfil de riesgo actual a todas las partes interesadas, incluyendo la efectividad del proceso de gestión de riesgos, la efectividad de los controles, diferencias, inconsistencias, redundancias, estado de la remediación y sus impactos en el perfil de riesgo.	MetricStream PowerBI	PC, impresora, sistema de almacenamiento en la red.	Encargado de soporte técnico

	Revisar los resultados de evaluaciones objetivas de terceras partes, auditorías internas y revisiones del aseguramiento de la calidad y mapearlos con el perfil de riesgo. Revisar las diferencias y exposiciones identificadas para determinar la necesidad de análisis de riesgos adicionales.	AuditoBoard MetricSteam Excel	PC, sistema de almacenamiento en la red.	Jefe de Unidad de TI, Encargado de soporte técnico

	De forma periódica, para áreas con un riesgo relativo y una paridad de capacidad del riesgo, identificar oportunidades relacionadas con TI que podrían permitir la aceptación de un mayor riesgo y un crecimiento y retorno mayores.	PowerBI Excel	PC, sistemas de respaldo de información.	Jefe de Unidad de TI

APO12.05 Definir un portafolio de acciones para la gestión de riesgos.

1. Mantener un inventario de actividades de control que estén en marcha para gestionar al riesgo y que permitan que el riesgo que se tome esté alineado con el apetito y tolerancia al riesgo. Clasificar las actividades de control y mapearlas con las declaraciones de riesgo específicas de TI y agrupaciones de riesgo de TI.

2. Determinar si cada entidad organizativa supervisa el riesgo y acepta la responsabilidad para operar dentro de sus niveles de tolerancia individuales y de portafolio.

3. Definir un conjunto de propuestas de proyecto equilibradas diseñadas para reducir el riesgo y/o proyectos que permitan oportunidades

estratégicas empresariales, considerando costes/beneficios, el efecto en el perfil de riesgo actual y las regulaciones.

Activos de Información			Activos Físicos	Activos Humanos
COD	Manejo de Información de TI	Software	Hardware	Personal
APO12.05	Mantener un inventario de actividades de control que estén en marcha para gestionar al riesgo y que permitan que el riesgo que se tome esté alineado con el apetito y tolerancia al riesgo. Clasificar las actividades de control y mapearlas con las declaraciones de riesgo específicas de TI y agrupaciones de riesgo de TI.	Archer Excel	PC, sistemas de respaldo de información, impresora.	Jefe de Unidad de TI, Encargado de soporte técnico

	Determinar si cada entidad organizativa supervisa el riesgo y acepta la responsabilidad para operar dentro de sus niveles de tolerancia individuales y de portafolio.	MetricStream PowerBI Word	PC, proyector, sistema de respaldo de información.	Jefe de Unidad de TI
	Definir un conjunto de propuestas de proyecto equilibradas diseñadas para reducir el riesgo y/o proyectos que permitan oportunidades estratégicas empresariales, considerando costes/beneficios, el efecto en el perfil de riesgo actual y las regulaciones.	Microsoft Project PowerPoint	PC, proyector, sistema de respaldo de información.	Jefe de Unidad de TI, Encargado de soporte técnico

APO12.06 Responder al riesgo.

1. Preparar, mantener y probar planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente con un impacto de negocio grave. Asegurar que los planes incluyan vías de escalado a través de la empresa.

2. Categorizar los incidentes y comparar las exposiciones reales con los umbrales de tolerancia al riesgo. Comunicar los impactos en el negocio a los responsables de toma de decisiones como parte de la notificación y actualizar el perfil de riesgo.

3. Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes de riesgo.

4. Examinar eventos adversos/pérdidas del pasado y oportunidades perdidas y determinar sus causas raíz. Comunicar la causa raíz, requerimientos de respuesta adicionales para el riesgo y mejoras de proceso a los responsables de toma de decisiones apropiados y asegurarse de que la causa, los requerimientos de respuesta y la mejora del proceso se incluyan en los procesos de gobierno del riesgo.

Activos de Información			Activos Físicos	Activos Humanos
COD	Manejo de Información de TI	Software	Hardware	Personal

APO12.06	Preparar, mantener y probar planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente con un impacto de negocio grave. Asegurar que los planes incluyan vías de escalado a través de la empresa.	**DRaaS** (Disaster Recovery as a Service) para planes de recuperación.	Servidor de respaldo, PC	Jefe de Unidad de TI, Encargado de soporte técnico

	Categorizar los incidentes y comparar las exposiciones reales con los umbrales de tolerancia al riesgo. Comunicar los impactos en el negocio a los responsables de toma de decisiones como parte de la notificación y actualizar el perfil de riesgo.	Splunk PowerBI Jira	PC, proyector, sistema de almacenamiento.	Jefe de Unidad de TI, Encargado de soporte técnico
	Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes de riesgo.	ServicesNow Slack PagerDuty	PC, sistema de respaldo de información	Encargado de soporte técnico

	Examinar eventos adversos/pérdidas del pasado y oportunidades perdidas y determinar sus causas raíz. Comunicar la causa raíz, requerimientos de respuesta adicionales para el riesgo y mejoras de proceso a los responsables de toma de decisiones apropiados y asegurarse de que la causa, los requerimientos de respuesta y la mejora del proceso se incluyan en los procesos de gobierno del riesgo.	PowerPoint Root Cuase Analizer	PC, proyector, sistema de almacenamiento.	Jefe de Unidad de TI

APO13 GESTIONAR LA SEGURIDAD

(Fernando Chevez)

APO13.01

1. Definir el alcance y los límites del SGSI en términos de las características de la empresa, la organización, su localización, activos y tecnología. Incluir detalles de y justificación para, cualquier exclusión del alcance.
2. Definir un SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología.
3. Alinear el SGSI con el enfoque global de la gestión de la seguridad en la empresa.
4. Obtener autorización de la dirección para implementar y operar o cambiar el SGSI.
5. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.
6. Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información.
7. Comunicar el enfoque de SGSI.

Activos de Información			Activos Físicos	Activos Humanos
COD	Manejo de Información de TI	Software	Hardware	Personal

APO13.01	Definir el alcance y los límites del SGSI en términos de las características de la empresa, la organización, su localización, activos y tecnología. Incluir detalles de y justificación para, cualquier exclusión del alcance.	Microsoft Visio, Word.	*PC* *Servidor de base de datos.*	*Jefe de Unidad de TI*
	Definir un SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología.	Sharepint	*PC* *Servidor de base de datos.*	*Jefe de Unidad de TI*
	Alinear el SGSI con el enfoque global de la gestión de la seguridad en la empresa.	RSA Archer Jira	*PC*	*Jefe de Unidad de TI*

	Obtener autorización de la dirección para implementar y operar o cambiar el SGSI.	DocuSign Microsoft Teams	*PC*	*Jefe de Unidad de TI*
	Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI	Microsoft Word	*Servidor de base de datos.*	*Jefe de Unidad de TI*
	Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información.	SAP SuccessFactors Microsoft Teams	*PC*	*Jefe de Unidad de TI*
	Comunicar el enfoque de SGSI.	PowerPoint	*Proyector*	*Encargado de Soporte Técnico*

APO13.02

1. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura de la empresa. Asegurar que el plan identifica las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, las responsabilidades y las prioridades asociadas para gestionar los riegos identificados de seguridad de información.

2. Mantener un inventario de componentes de la solución implementados para gestionar los riesgos relacionados con la seguridad como parte de la arquitectura de la empresa.

3. Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información, sustentados en casos de negocio adecuados que incluyan consideren la financiación la asignación de roles y responsabilidades.

4. Proporcionar información para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas en base al plan de tratamiento de riesgos de seguridad de información.

5. Definir la forma de medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizar estas mediciones para evaluar la efectividad y producir resultados reproducibles y comparables.

6. Recomendar programas de formación y concienciación en seguridad de la información.

7. Integrar la planificación, el diseño, la implementación y la supervisión de los procedimientos de seguridad de información y otros controles que permitan la prevención y detección temprana de eventos de seguridad, así como la respuesta a incidentes de seguridad.

Activos de Información			Activos Físicos	Activos Humanos
COD	Manejo de Información de TI	Software	Hardware	Personal

APO13.02	Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura de la empresa. Asegurar que el plan identifica las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, las responsabilidades y las prioridades asociadas para gestionar los riegos identificados de seguridad de información.	MetricStream Microsoft Excel	PC Servidor de base de datos.	*Jefe de Unidad de TI*

	Mantener un inventario de componentes de la solución implementados para gestionar los riesgos relacionados con la seguridad como parte de la arquitectura de la empresa.	SolarWinds Asset Management	PC Servidor de base de datos.	Encargado de Soporte Técnico
	Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información, sustentados en casos de negocio adecuados que incluyan consideren la financiación la asignación de roles y responsabilidades.	Microsoft Project Tableau	PC	Jefe de Unidad de TI

	Proporcionar información para el diseño y desarrollo de prácticas de gestión y soluciones seleccionadas en base al plan de tratamiento de riesgos de seguridad de información.	Jira Fortinet	Firewall FortiGate	Encargado de Soporte Técnico
	Definir la forma de medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizar estas mediciones para evaluar la efectividad y producir resultados reproducibles y comparables.	Splunk Grafana	Servidor de monitoreo dedicado para recolectar y analizar datos de seguridad.	Jefe de Unidad de TI
	Recomendar programas de formación y concienciación en seguridad de la información.	Moodle Microsoft Teams	PC Dispositivos móviles	Encargado de Soporte Técnico

	Integrar la planificación, el diseño, la implementación y la supervisión de los procedimientos de seguridad de información y otros controles que permitan la prevención y detección temprana de eventos de seguridad, así como la respuesta a incidentes de seguridad.	IBM QRadar Microsft Azure	Servidor con IDS	Encargado de Soporte Técnico

APO13.03

1. Realizar revisiones periódicas del SGSI, incluyendo aspectos de políticas, objetivos y prácticas de seguridad del SGSI. Considerar los resultados de auditorías de seguridad, incidentes, resultados de mediciones de efectividad, sugerencias y retroalimentación de todas las partes interesadas.

2. Realizar auditorías internas al SGSI a intervalos planificados.

3. Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.

4. Proporcionar información para el mantenimiento de los planes de seguridad para que consideren las incidencias de las actividades de supervisión y revisión periódica.

5. Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.

Activos de Información			Activos Físicos	Activos Humanos
COD	Manejo de Información de TI	Software	Hardware	Personal
APO13.02	Realizar revisiones periódicas del SGSI, incluyendo aspectos de políticas, objetivos y prácticas de seguridad del SGSI. Considerar los resultados de auditorías de seguridad, incidentes, resultados de mediciones de efectividad, sugerencias y retroalimentación de todas las partes interesadas.	Compliance Manager Confluence	Servidor con base de datos	Jefe de Unidad de TI

	Realizar auditorías internas al SGSI a intervalos planificados.	TeamMate Audit	PC	Jefe de Unidad de TI
	Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.	Power BI Microsoft Teams	PC Proyector	Jefe de Unidad de TI
	Proporcionar información para el mantenimiento de los planes de seguridad para que consideren las incidencias de las actividades de supervisión y revisión periódica.	Microsoft Word y Excel	Servidor de Base de datos	Jefe de Unidad de TI
	Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.	LogRhythm Splink	Servidor de Base de datos	Encargado de Soporte Técnico

4.7 MATRIZ DE RIESGO DE LOS PROCESOS.

EDM03 – Asegurar la Optimización del Riesgo

MATRIZ DE RIESGOS
ID PROYECTO:
FECHA DE INICIO: 11 de noviembre de 2024
FECHA DE TÉRMINO PROPUESTA: 8 de diciembre de 2024

#	Proceso	Tipo de Riesgo	Riesgo	Posible Resultado (entonces)	Síntoma	Probabilidad	Impacto	Nivel de Prioridad	EVALUACIÓN		Estrategia	Respuesta	Responsable de la acción de respuesta
									Valor	Nivel			
1	EDM03 - Asegurar la Optimización del Riesgo	Operaciones	Falta de actualización en los planes de respuesta ante incidentes	Retraso en la reacción a incidentes críticos, aumentando el impacto en las operaciones	Duplicación de controles, fallos en la cobertura de riesgo	2	3	6	1	ALTO	EVITAR	Revisar y optimizar el marco de gestión de riesgos periódicamente para eliminar redundancias y asegurar su efectividad.	Jefe de Operaciones
2		Informática	Fallos en el hardware crítico, como UPS o servidores de respaldo	Pérdida de datos, interrupción del servicio y falla en la continuidad del negocio	Lentitud en el procesamiento de datos de riesgo, frecuentes fallos del sistema	3	3	9	1	ALTO	EVITAR	Actualizar o reemplazar tecnología según un análisis coste-beneficio para mejorar la eficiencia en la gestión del riesgo.	Jefe de TI
3		Contabilidad	Gastos elevados en la implementación de controles y proyectos de mitigación sin un análisis adecuado de coste/beneficio	Sobrecostos que afectan el presupuesto asignado para otros proyectos y operaciones	Lentitud en el procesamiento de datos de riesgo, frecuentes fallos del sistema	2	3	6	1	ALTO	EVITAR	Realizar análisis de coste-beneficio para equilibrar el gasto en medidas de mitigación con el impacto real en la reducción del riesgo.	Jefe de contabilidad

APO12 – Gestionar el riesgo. (Javier Mejía)

MATRIZ DE RIESGOS
ID PROYECTO:
FECHA DE INICIO: 11 de noviembre de 2024
FECHA DE TÉRMINO PROPUESTA: 8 de diciembre de 2024

#	Proceso	Tipo de Riesgo	Riesgo	Posible Resultado (entonces)	Síntoma	Probabilidad	Impacto	Nivel de Prioridad	EVALUACIÓN		Estrategia	Respuesta	Responsable de la acción de respuesta
									Valor	Nivel			
1	APO12 - Gestionar el Riesgo	Operaciones	Falta de actualización en los planes de respuesta ante incidentes	Retraso en la reacción a incidentes críticos, aumentando el impacto en las operaciones	Documentación desactualizada, procedimientos de respuesta no reflejan los cambios recientes en la infraestructura	2	3	6	1	ALTO	EVITAR	Actualizar y revisar regularmente los planes de respuesta.	Jefe de Operaciones
2		Informática	Fallos en el hardware crítico, como UPS o servidores de respaldo	Pérdida de datos, interrupción del servicio y falla en la continuidad del negocio	Alertas de fallos de hardware, inestabilidad en el sistema, lentitud en la recuperación	3	3	9	1	ALTO	EVITAR	Implementar redundancia y realizar mantenimientos preventivos en el hardware.	Jefe de TI
3		Contabilidad	Gastos elevados en la implementación de controles y proyectos de mitigación sin un análisis adecuado de coste/beneficio	Sobrecostos que afectan el presupuesto asignado para otros proyectos y operaciones	Desviación presupuestaria, falta de fondos para otros proyectos críticos	2	3	6	1	ALTO	EVITAR	Realizar análisis de coste-beneficio antes de implementar controles adicionales.	Jefe de contabilidad

APO13 – Gestionar la Seguridad. (Fernando Chevez)

MATRIZ DE RIESGOS
ID PROYECTO:
FECHA DE INICIO: 11/11/2024
FECHA DE TÉRMINO PROPUESTA: 08/12/2024

#	Proceso	Tipo de Riesgo	Riesgo	Posible Resultado (entonces)	Síntoma	Probabilidad	Impacto	Nivel de Prioridad	EVALUACIÓN		Estrategia	Respuesta	Responsable de la acción de respuesta
									Valor	Nivel			
1	APO13-Gestión de la Seguridad	**Area de Salon**	Incendio en el local	Perdida de equipo información y la información almacenada en ella.	Se percibe un olor de cableado eléctrico quemado.	2	3	6	3	Alto	Evitar	Monitoreo de las tensiones eléctricas generadas y compra de equipo que evite la sobrecarga.	Jefe de la Unidad de TI
2		**Recursos Humanos**	Robo de credenciales a personal.	Información importante de la empresa comprometida.	Inicios de sesión de personal de dispositivos desconocidos y en horarios irregulares.	2	3	6	3	Alto	Evitar	Capacitación al personal sobre la seguridad digital y un monitoreo controlado de acceso.	Personal
3		**Area de TI**	Ataques cibernéticos.	Robo de información y fallos en los servicios.	Rendimiento lento del sistema o esté interrumpido en su totalidad.	3	3	9	3	Alto	Evitar	Monitoreo constante del sistema, uso de antivirus y firewall, autenticación multifactor y politicas de seguridad bien definidas.	Jefe de la Unidad de TI

4.8 POLITICAS DEL PLAN DE MEJORA.

EDM03 Asegurar la optimización del riesgo (Fátima Ayala)

- Política de revisión y optimización del marco de gestión de riesgos.
- Política de actualización o reemplazo de tecnología según análisis coste-beneficio.
- Política de análisis coste-beneficio para medidas de mitigación de riesgos.

APO12 Gestionar el riesgo. (Javier Mejía)

- Política de Actualización y revisión regular de los planes de respuesta.
- Política de implementación de redundancia y realización de mantenimientos preventivos de hardware.
- Política de realización de análisis coste-beneficio.

APO13 – Gestionar la Seguridad. (Fernando Chevez)

- Política de monitoreo de las tensiones eléctricas generadas y compra de equipo que evite la sobrecarga.
- política de capacitación al personal sobre la seguridad digital y un monitoreo controlado de acceso.
- política de capacitación al personal sobre la seguridad digital y un monitoreo controlado de acceso.

4.8.1 POLITICAS A IMPLEMENTAR.

EDM03 Asegurar la optimización del riesgo (Fátima Ayala)

A) Política de revisión y optimización del marco de gestión de riesgos.

1. **Objetivo General:**

Garantizar que el marco de gestión de riesgos sea efectivo y esté alineado con los objetivos estratégicos de FLERT SALON & SPA, a través de revisiones periódicas que eliminen redundancias y mejoren su eficiencia.

2. **Alcance:**

La política aplica a todos los procesos, sistemas y actividades relacionadas con la gestión de riesgos dentro de FLERT SALON & SPA , incluyendo a los responsables de TI y demás áreas implicadas.

3. **Lineamientos**

- ✓ Realizar una revisión anual del marco de gestión de riesgos para ajustarlo a nuevas normativas, cambios tecnológicos o amenazas emergentes.
- ✓ Eliminar redundancias en los procesos para maximizar la eficiencia operativa.
- ✓ Involucrar a los responsables de TI y otras áreas clave en el análisis y optimización del marco de gestión.

4. **Herramientas**

- **ISO 31000**: Proporciona un marco estándar para la gestión de riesgos.
- **Software GRC**: Herramientas como RSA Archer o LogicManager facilitan la evaluación y el seguimiento de riesgos.

B) Política de actualización o reemplazo de tecnología según análisis coste-beneficio.

1. **Objetivo General**

Asegurar que la tecnología empleada en FLERT SALON & SPA sea eficiente y acorde a las necesidades del negocio, justificando cada decisión a través de un análisis coste-beneficio que permita una inversión estratégica.

2. **Alcance**

Esta política aplica a toda la infraestructura tecnológica de FLERT SALON & SPA, incluyendo hardware, software, redes y servicios digitales, abarcando las áreas operativas y administrativas de la empresa.

3. **Lineamientos**

- ✓ Evaluar periódicamente la tecnología existente para identificar posibles obsolescencias o deficiencias.
- ✓ Realizar un análisis costo-beneficio antes de implementar actualizaciones o adquirir nuevas tecnologías.
- ✓ Seleccione tecnologías que, además de cubrir las necesidades actuales, sean escalables para el futuro crecimiento de la empresa.

4. Herramientas

- **ROI Calculator Tools**: Para calcular el retorno sobre la inversión de posibles adquisiciones tecnológicas.
- **Plataformas de evaluación tecnológica**: Gartner o Forrester para analizar tendencias y opciones de herramientas.

C) Política de análisis coste-beneficio para medidas de mitigación de riesgos.

1. Objetivo General:

Equilibrar el gasto en medidas de mitigación con su impacto real en la reducción de riesgos, maximizando la eficiencia de los recursos asignados para proteger las operaciones de FLERT SALON & SPA.

2. Alcance:

Aplica a todas las decisiones relacionadas con la implementación de controles y medidas de mitigación de riesgos dentro del área de TI, así como las operaciones administrativas y de servicio al cliente de FLERT SALON & SPA.

3. Lineamientos:

- ✓ Priorizar riesgos críticos según su impacto y probabilidad, asegurando que los recursos se destinen a las áreas más relevantes.
- ✓ Realizar un análisis coste-beneficio detallado para justificar la implementación de controles o medidas preventivas.

- ✓ Evaluar periódicamente la efectividad de las medidas implementadas, ajustándolas según sea necesario para mantener su rentabilidad.

4. **Herramientas:**

- **RiskLens:** Para analizar el impacto financiero de los riesgos de manera cuantitativa.
- **BowTieXP:** Herramienta que permite visualizar riesgos y medidas de mitigación en diagramas claros y comprensibles.

APO12 Gestionar el riesgo. (Javier Mejía)

A) Política de Actualización y revisión regular de los planes de respuesta.

1. **Objetivo General:**

Optimizar la capacidad de Flert SALON & SPA para responder a incidentes críticos, minimizando el impacto sobre las operaciones y mejorando la resiliencia organizacional mediante la actualización y revisión continua de los planes de respuesta.

2. **Alcance:**

Esta política abarca todas las áreas de operación de Flert SPA & SALON, incluyendo servicios al cliente, operaciones administrativas y sistemas de TI. Se dirige principalmente a fortalecer los procedimientos ante situaciones de emergencia, incidentes de seguridad y desastres naturales.

3. **Lineamientos:**

- ✓ Revisar los planes de respuesta al menos una vez cada seis meses o cada vez que ocurran cambios significativos en la infraestructura o personal.
- ✓ Incluir la participación de los líderes de cada departamento en la revisión para asegurar la relevancia y efectividad del plan en todos los sectores.

- ✓ Realizar simulacros de respuesta para evaluar la efectividad del plan y ajustar los protocolos según los resultados de los ensayos.

4. **Herramientas.**

- **Asana:** Para la gestión de tareas relacionadas con las revisiones y actualizaciones.
- **Slack:** Para la comunicación rápida y efectiva entre equipos durante la implementación de cambios.
- **Suite de Office:** Para la documentación colaborativa y almacenamiento de los planes actualizados.

B) Política de implementación de redundancia y realización de mantenimientos preventivos de hardware.

1. **Objetivo General:**

Asegurar la continuidad operativa de Flert SALON & SPA mediante la implementación de redundancias en sistemas críticos y la ejecución de mantenimientos preventivos regulares en el hardware.

2. **Alcance:**

Esta política incluye todos los dispositivos y sistemas de hardware utilizados en Flert SALON & SPA, tales como computadoras de administración, servidores y sistemas de control de inventario. Busca garantizar la disponibilidad continua y el funcionamiento óptimo de los equipos esenciales.

3. **Lineamientos:**

- ✓ Identificar los puntos críticos donde es necesaria la redundancia, especialmente en dispositivos que sostienen la operación diaria de Flert SALON & SPA.
- ✓ Programar mantenimientos preventivos trimestrales para reducir el riesgo de fallos imprevistos y prolongar la vida útil del hardware.

- ✓ Llevar un registro detallado de cada mantenimiento y actualización, así como de los reemplazos de hardware necesarios para asegurar una trazabilidad de las acciones realizadas.

4. **Herramientas.**
    - **Nagios:** Para la monitorización continua de hardware crítico.
    - **HD Sentinel:** Para verificar el estado de los discos duros.
    - **AnyDesk:** Para el soporte técnico remoto en el mantenimiento de hardware.
    - **ERPNext:** Para el registro y programación de mantenimientos preventivos.
    - **Microsoft Excel:** Para la elaboración de cronogramas de mantenimiento y registros manuales en caso de necesidad.

C) Política de realización de análisis coste-beneficio.

1. **Objetivo General:**

Evaluar la rentabilidad y efectividad de los controles adicionales propuestos para Flert SALON & SPA, a fin de asegurar que cada inversión en seguridad o infraestructura aporte un valor real y optimice los recursos de la empresa.

2. **Alcance:**

El análisis de coste-beneficio se aplicará a cualquier propuesta de control adicional que impacte en la infraestructura tecnológica, seguridad o servicios al cliente de Flert SALON & SPA. Su enfoque es seleccionar aquellas medidas que aporten el máximo beneficio con el menor costo posible.

3. **Lineamientos:**

- ✓ Establecer criterios específicos para el análisis, como costo, impacto en la seguridad, mejora en la productividad y satisfacción del cliente.
- ✓ Consultar a los líderes de cada área involucrada para conocer la relevancia de los controles propuestos en el contexto operativo y financiero.

- ✓ Documentar los resultados del análisis y someter la decisión de implementación a la aprobación de la gerencia, considerando el balance entre costos y beneficios para cada control.

4. **Herramientas.**
   - **Microsoft Excel:** Para el cálculo de costos y beneficios, incluyendo gráficos y tablas comparativas.
   - **Power BI:** Para la visualización y análisis avanzado de datos financieros.
   - **QuickBooks:** Para obtener datos contables y financieros necesarios para los análisis.

APO13 – Gestionar la Seguridad. (Fernando Chevez)

A) Política de monitoreo de las tensiones eléctricas generadas y compra de equipo que evite la sobrecarga.

1. Objetivo general

Garantizar la seguridad de las instalaciones y de la información almacenada, previniendo incendios mediante la gestión y monitoreo de riesgos eléctricos en los salones de FLERT SALON & SPA.

2. Alcance

Esta política aplica a todas las unidades y áreas operativas en los salones de FLERT SALON & SPA que utilicen equipos eléctricos y de cómputo.

3. Lineamientos

- ✓ Realizar monitoreo constante de las tensiones eléctricas y mantenimiento del cableado.
- ✓ Evitar la sobrecarga de circuitos eléctricos; implementar un sistema de control y estabilización de carga.

- ✓ Instalar detectores de humo y tener extintores accesibles y en buen estado.
- ✓ Capacitar al personal en la identificación de posibles riesgos eléctricos y en el uso adecuado de extintores.

4. Herramienta para esta política:

Se recomienda utilizar dispositivos de monitoreo eléctrico como polímetros y realizar inspecciones semestrales del sistema eléctrico, además de actualizar las herramientas de monitoreo cada año.

B) Política de capacitación al personal sobre la seguridad digital y un monitoreo controlado de acceso.

1. Objetivo general

Proteger la integridad de la información y prevenir el robo de credenciales mediante prácticas de seguridad y capacitación del personal de FLERT SALON & SPA.

2. Alcance

Esta política es aplicable a todo el personal de FLERT SALON & SPA que tenga acceso a sistemas de información y datos de la empresa.

3. Lineamientos

- ✓ Capacitar al personal en la importancia de la seguridad digital y manejo seguro de credenciales.
- ✓ Prohibir el uso de contraseñas débiles y fomentar la autenticación multifactor para accesos críticos.
- ✓ Implementar un sistema de monitoreo de accesos y alertas para actividades inusuales.

- ✓ Exigir cambios periódicos de contraseñas y limitar el acceso a información sensible a solo el personal autorizado.

4. Herramienta para esta política

Se sugiere utilizar un gestor de contraseñas y autenticación multifactor, revisando y actualizando el sistema cada seis meses.

C) Política de monitoreo constante del sistema, uso de antivirus y firewall, autenticación multifactor y reglas de seguridad bien definidas.

1. Objetivo general

Prevenir ataques cibernéticos y proteger los sistemas informáticos de FLERT SALON & SPA mediante la implementación de medidas de seguridad y protocolos de respuesta ante incidentes.

2. Alcance

Aplica a todos los sistemas y equipos informáticos utilizados en las operaciones de FLERT SALON & SPA, incluyendo servidores, redes y dispositivos conectados.

3. Lineamientos

- ✓ Instalar y actualizar regularmente software antivirus y firewall en todos los dispositivos de la red.
- ✓ Prohibir la instalación de software sin autorización en los equipos de la empresa.
- ✓ Realizar auditorías de seguridad trimestrales y monitoreo constante de posibles amenazas.

- ✓ En caso de un incidente de seguridad, seguir el procedimiento de desconexión de la red, análisis de amenazas y recuperación de sistemas afectados.

4. Herramienta para esta política

Utilizar herramientas de monitoreo de seguridad y realizar escaneos de amenazas semanalmente; actualizar los sistemas de seguridad de acuerdo con nuevas amenazas cada tres meses.

4.8.2 BENEFICIOS/COSTOS QUE OBTENDRIA CON LA IMPLEMENTACIÓN DEL MODELO GOBIERNO Y GESTION DE TI.

EDM03 Asegurar la optimización del riesgo (Fátima Ayala)

Beneficios.

1. Gestione riesgos de manera eficiente y estratégica, reduciendo el impacto de posibles amenazas.
2. Optimice sus recursos tecnológicos y financieros, incrementando la rentabilidad.
3. Aumente su resiliencia ante cambios externos en el entorno tecnológico y empresarial.
4. Fomente una cultura de mejora continua, posicionando a la empresa como moderna y adaptativa en un mercado competitivo.

Costos

CATEGORIA	DESCRIPCIÓN	COSTO
HUMANO	Jefe de Unidad de TI	Ya se cuenta con este empleado.
	Encargado de soporte técnico.	Ya se cuenta con este empleado.
SOFTWARE	LogicManager	$ 833.33
	RiskLens	$ 300.00

HARDWARE	Actualización o Mantenimiento de Servidores	$ 2,000
OTROS	Consultoría Externa	$1,000
TOTAL		$4.133.33

APO12. Gestionar el riesgo. (Javier Mejía)

Beneficios.

1. Mejora en la coordinación y respuesta ante emergencias, reduciendo interrupciones en las operaciones de Flert SALON & SPA.
2. Prolongación de la vida útil de los equipos y disminución de costos asociados a fallas imprevistas mediante mantenimientos preventivos.
3. Optimización de recursos gracias a la toma de decisiones informadas basada en análisis de coste-beneficio.
4. Mayor claridad en responsabilidades y procesos, promoviendo una comunicación efectiva y cumplimiento de estándares.
5. Reducción del riesgo operativo mediante la implementación de redundancias y planes actualizados.

Costos:

CATEGORIA	DESCRIPCIÓN	COSTO
HUMANO	Encargado de soporte técnico.	Ya se cuenta con este empleado.
	Auditor Interno	Ya se cuenta con este empleado.
	Contador	Ya se cuenta con este empleado.
SOFTWARE	Licencia Trello	$ 30.00
	Power BI	$ 17.00
HARDWARE	UPS	$ 204.00

	Bobina de cable UTP	$ 142.00
OTROS	Impresión y documentación de planes de respuesta	$ 100.00
TOTAL		$ 493.00

APO13 – Gestionar la Seguridad. (Fernando Chevez)

Beneficios

1. Establecer una seguridad robusta que minimice el impacto de posibles riesgos operativos y tecnológicos en las operaciones de FLERT.
2. Proteger la integridad y disponibilidad de los activos críticos, incluyendo datos y sistemas de información.
3. Fortalecer la confianza de los clientes mediante la implementación de prácticas de seguridad efectivas y transparentes.
4. Reducir los costos asociados a incidentes de seguridad, aumentando la eficiencia operativa y tecnológica.
5. Asegurar el cumplimiento normativo y evitar sanciones legales o regulatorias.

CATEGORIA	DESCRIPCIÓN	COSTO
HUMANO	Jefe de Unidad de Seguridad TI	$1,200.00
	Encargado de monitoreo de eléctrico.	$800.00
SOFTWARE	Antivirus empresarial: ESET.	$1,000.00
	Firewall: Sophos XG y IDS: Snort	$1,500.00

HARDWARE	Detectores de sobrecarga eléctrica	$2,000.00
CONSULTORÍA	Auditoría externa para identificar vulnerabilidades	$1,500.00
CAPACITACIÓN	Formación para el personal en seguridad digital	$800.00
TOTAL		$10,500.00

CONCLUSIONES.

En el primer capítulo se presenta una visión integral de la empresa, destacando su misión, visión, valores y los objetivos estratégicos que guían sus operaciones. Se describe la estructura organizativa, incluyendo la gobernabilidad interna y el rol clave de la unidad de TI, cuyo posicionamiento es fundamental para apoyar los procesos de la empresa. La descripción de los recursos tecnológicos y sistemas de información subraya la importancia del área de TI en la consecución de los objetivos empresariales. El análisis FODA realizado proporciona una comprensión clara de las fortalezas, oportunidades, debilidades y amenazas, tanto a nivel institucional como en la unidad de TI, estableciendo una base sólida para la aplicación de marcos de gestión como COBIT 5.0 en los siguientes capítulos. Este análisis permitirá alinear de manera efectiva las estrategias empresariales con las capacidades tecnológicas, facilitando una gobernanza y gestión óptima de la TI.

COBIT 5.0 proporciona un marco robusto y estructurado para la gobernanza y gestión de TI, ofreciendo directrices y mejores prácticas que ayudan a las organizaciones a alinear sus iniciativas de TI con los objetivos estratégicos del negocio. La metodología de COBIT 5.0 no solo se centra en la optimización de recursos y la reducción de riesgos, sino que también mejora la calidad

de los servicios de TI, asegura el cumplimiento normativo y fortalece la seguridad de la información.

El capítulo III resalta la importancia de la aplicación de COBIT 5.0 para alinear la gobernanza y gestión de TI con los objetivos estratégicos de la empresa. Se identifican las áreas clave donde la tecnología puede optimizar procesos y apoyar la operación del negocio. La auditoría asegura que las necesidades de las partes interesadas estén cubiertas y que las decisiones en TI se tomen de forma informada y eficiente. Se evidencia la necesidad de una integración total del marco COBIT 5.0 en todos los niveles organizacionales, no solo en el área de TI, lo cual permitirá maximizar los beneficios tecnológicos, mejorar la seguridad y garantizar el cumplimiento normativo.

El análisis y desarrollo de los procesos EDM03, APO12 y APO13 han permitido establecer un enfoque sistemático y estructurado para gestionar los riesgos y la seguridad en FLERT SALON & SPA, fortaleciendo la gobernanza y asegurando la continuidad operativa de la organización. La implementación de estas prácticas no solo optimiza la respuesta ante eventos adversos, sino que también mejora la toma de decisiones estratégicas al alinear los riesgos con los objetivos empresariales.

RECOMENDACIONES.

Es fundamental que FLERT SALON & SPA continúe fortaleciendo su infraestructura tecnológica y su Unidad de TI para asegurar que esté alineada con los objetivos estratégicos de la empresa. Dado que la TI es un pilar importante para el soporte de las operaciones diarias y la eficiencia en el servicio al cliente, se recomienda invertir en actualizaciones tecnológicas constantes y en la capacitación del personal. Estas mejoras contribuirán a una mayor eficiencia operativa y garantizarán la competitividad a largo plazo de la empresa en un entorno cada vez más digitalizado.

Se recomienda que FLERT SALON & SPA adopte un enfoque más holístico en la implementación de COBIT 5.0, asegurando que todas las áreas de la organización, no solo el área de TI, estén involucradas en la gestión y gobernanza tecnológica. Además, sería beneficioso realizar evaluaciones periódicas del nivel de madurez en TI para identificar áreas de mejora y asegurar un cumplimiento adecuado con las normativas y estándares internacionales. Este enfoque garantizará que los beneficios de COBIT 5.0 se maximicen, optimizando recursos y reduciendo riesgos operativos.

Se sugiere que FLERT SALON & SPA dirija sus esfuerzos a mejorar la alineación entre las necesidades de las partes interesadas y los objetivos estratégicos de TI. Esto puede lograrse optimizando la gobernanza y gestión de TI mediante la metodología COBIT 5.0. Es fundamental asegurar que todos los procesos de TI estén claramente definidos y alineados con las metas del negocio. También es esencial que la empresa garantice la disponibilidad de los recursos necesarios, tanto humanos como tecnológicos, para la correcta implementación de las mejoras identificadas durante la auditoría. Además, se aconseja mantener un control riguroso del tiempo y los recursos financieros asignados a estas iniciativas para asegurar su éxito y cumplimiento dentro de los plazos establecidos.

Para garantizar un entorno operativo seguro, es recomendable que FLERT SALON & SPA implemente un enfoque integral en la gestión de riesgos y seguridad de la información, alineando sus procesos con el marco COBIT 5.0 para optimizar la eficiencia operativa y proteger sus activos críticos. Esto incluye la capacitación continua del personal en prácticas de seguridad, la adopción de tecnologías avanzadas para el monitoreo y la evaluación de riesgos, y la revisión periódica de políticas y procedimientos. Al fomentar una cultura de mejora continua y asegurar la participación de todos los empleados, la empresa podrá fortalecer su resiliencia ante amenazas y garantizar un entorno operativo seguro y eficiente.

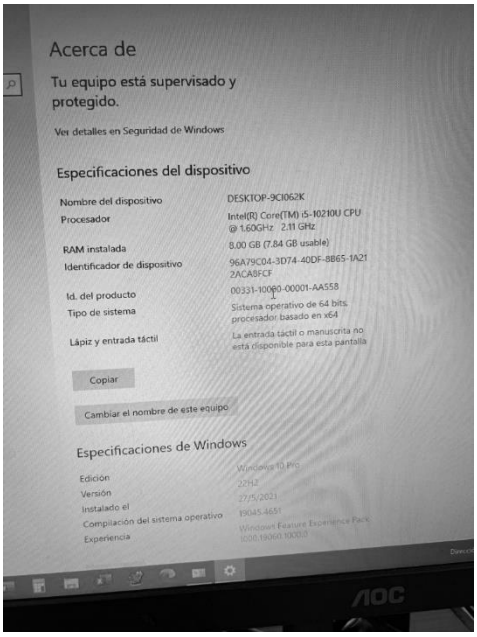
BIBLIOGRAFÍAS.

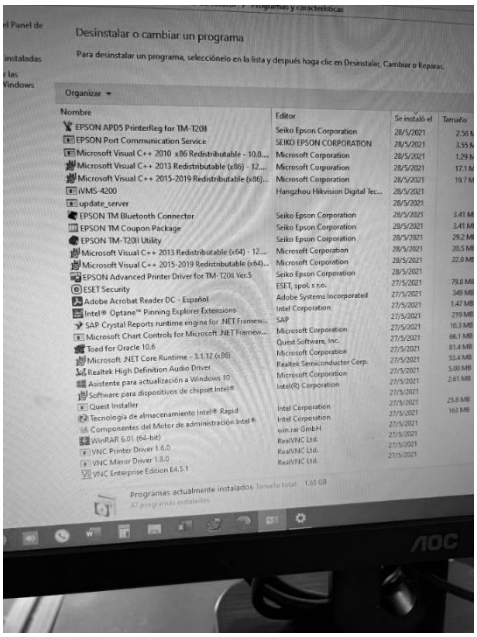
Asociación Española por la Calidad. (2024, 1 abril). *COBIT - AEC*. AEC. https://www.aec.es/conocimiento/centro-del-conocimiento/cobit/

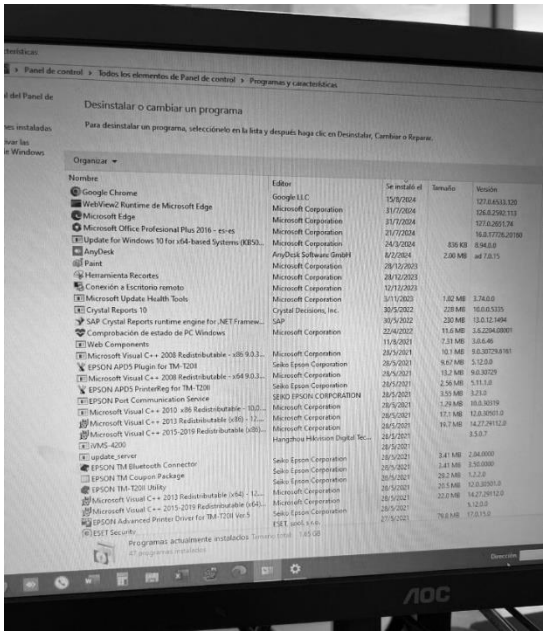
Asia, I. S. (2024, 24 Abril). What is COBIT (Control Objectives for Information and Related Technology)? *Information Security Asia*. https://informationsecurityasia.com/es/what-is-cobit-control-objectives-for-information-and-related-technology/#Benefits_of_Implementing_COBIT

Los cinco principios de COBIT 5 | Conexión ESAN. (s. f.). https://www.esan.edu.pe/conexion-esan/los-cinco-principios-de-cobit-5

ANEXOS


Acerca de
Tu equipo está supervisado y protegido.
Ver detalles en Seguridad de Windows
Especificaciones del dispositivo
Nombre del dispositivo
DESKTOP-9CI062K
Procesador
Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz 2.11 GHz
RAM instalada
8,00 GB (7,84 GB usable)
Identificador de dispositivo
96A79C04-3D74-40DF-8B65-1A212ACA8FCF
Id. del producto
00331-10000-00001-AA558
Tipo de sistema
Sistema operativo de 64 bits, procesador basado en x64
Lápiz y entrada táctil
La entrada táctil o manuscrita no está disponible para esta pantalla
Copiar
Cambiar el nombre de este equipo
Especificaciones de Windows
Edición
Windows 10 Pro
Versión
22H2
Instalado el
27/5/2021
Compilación del sistema operativo
19045.4651
Experiencia
Windows Feature Experience Pack 1000.19060.1000.0


Desinstalar o cambiar un programa
Para desinstalar un programa, selecciónelo en la lista y después haga clic en Desinstalar, Cambiar o Reparar.
Organizar
Nombre
Editor
Se instaló el
Tamaño
EPSON APD5 PrinterReg for TM-T20II
EPSON Port Communication Service
Microsoft Visual C++ 2010 x86 Redistributable - 10.0....
Microsoft Visual C++ 2013 Redistributable (x86) - 12....
Microsoft Visual C++ 2015-2019 Redistributable (x86)...
iVMS-4200
update_server
EPSON TM Bluetooth Connector
EPSON TM Coupon Package
EPSON TM-T20II Utility
Microsoft Visual C++ 2013 Redistributable (x64) - 12....
Microsoft Visual C++ 2015-2019 Redistributable (x64)...
EPSON Advanced Printer Driver for TM-T20II Ver.5
ESET Security
Adobe Acrobat Reader DC - Español
Intel® Optane™ Pinning Explorer Extensions
SAP Crystal Reports runtime engine for .NET Framew...
Microsoft Chart Controls for Microsoft .NET Framew...
Toad for Oracle 10.6
Microsoft .NET Core Runtime - 3.1.12 (x86)
Realtek High Definition Audio Driver
Asistente para actualización a Windows 10
Software para dispositivos de chipset Intel®
Quest Installer
Tecnología de almacenamiento Intel® Rapid
Componentes del Motor de administración Intel®
WinRAR 6.01 (64-bit)
VNC Printer Driver 1.6.0
VNC Mirror Driver 1.8.0
VNC Enterprise Edition E4.5.1
Programas actualmente instalados
47 programas instalados


Panel de control › Todos los elementos de Panel de control › Programas y características
Desinstalar o cambiar un programa
Para desinstalar un programa, selecciónelo en la lista y después haga clic en Desinstalar, Cambiar o Reparar.
Organizar
Nombre
Editor
Se instaló el
Tamaño
Versión
Google Chrome
WebView2 Runtime de Microsoft Edge
Microsoft Edge
Microsoft Office Profesional Plus 2016 - es-es
Update for Windows 10 for x64-based Systems (KB5...
AnyDesk
Paint
Herramienta Recortes
Conexión a Escritorio remoto
Microsoft Update Health Tools
Crystal Reports 19
SAP Crystal Reports runtime engine for .NET Framew...
Comprobación de estado de PC Windows
Web Components
Microsoft Visual C++ 2008 Redistributable - x86 9.0.3...
EPSON APD5 Plugin for TM-T20II
Microsoft Visual C++ 2008 Redistributable - x64 9.0.3...
EPSON APD5 PrinterReg for TM-T20II
EPSON Port Communication Service
Microsoft Visual C++ 2010 x86 Redistributable - 10.0....
Microsoft Visual C++ 2013 Redistributable (x86) - 12....
Microsoft Visual C++ 2015-2019 Redistributable (x86)...
iVMS-4200
update_server
EPSON TM Bluetooth Connector
EPSON TM Coupon Package
EPSON TM-T20II Utility
Microsoft Visual C++ 2013 Redistributable (x64) - 12....
Microsoft Visual C++ 2015-2019 Redistributable (x64)...
EPSON Advanced Printer Driver for TM-T20II Ver.5
ESET Security
Programas actualmente instalados
47 programas instalados

Enlace al instrumento de evaluación de necesidades de las partes interesadas en FLERT SALON & SPA: Instrumento de Evaluación

Enlace al documento Mapeo de Metas: MAPEO DE METAS.xlsx

Enlace a grabación de la reunión para asignación de punto en Mapeo de Metas: Reunión - Documento de Mapeo de Metas

Enlace a grabación de la reunión sobre habilitadores de COBIT 5.0: Habilitadores de COBIT 5.0.mp4

Enlace a documento de Evaluación Técnica de Procesos.

EVALUACIÓN TECNICA DE PROCESOS.xlsx

Enlaces a documento de Matriz de riesgos bajo la línea del PMI.

MATRIZ DE RIESGO BAJO LA LINEA DEL PMI (EDM03)

MATRIZ DE RIESGO BAJO LA LINEA DEL PMI (APO12 - Gestionar el riesgo).xlsx

MATRIZ DE RIESGO BAJO LA LINEA DEL PMI (APO13)