Contenido

Introducción

El presente proyecto empresarial tiene como propósito desarrollar una propuesta tecnológica enfocada en el diseño, administración y operación de redes de comunicación mediante la empresa HollyGather.

A través de este trabajo se integran conocimientos adquiridos en los diferentes módulos de formación, aplicando aspectos relacionados con telecomunicaciones, normatividad informática, seguridad de la información, emprendimiento, desarrollo web y difusión digital.

La creación de HollyGather surge de la necesidad de ofrecer soluciones de conectividad confiables y eficientes que permitan mejorar la comunicación entre personas, organizaciones y comunidades. Mediante el análisis de infraestructura tecnológica, diseño de servicios y aplicación de buenas prácticas empresariales, se busca demostrar cómo una empresa especializada en redes puede contribuir al desarrollo tecnológico actual.

Este proyecto representa la integración de conocimientos teóricos y prácticos, permitiendo fortalecer competencias profesionales relacionadas con el sector de las telecomunicaciones y las tecnologías de la información.

Misión

Desarrollar solución tecnológicas innovación que optimicen la interacción digital y la gestión de información de nuestros clientes.

Visión

Ser una empresa referente a la creación de ecosistemas tecnológicos funcional, confiables y personalizados que impulsan el crecimiento y la eficiencia de cada organización.

Valores

. Innovación

. Compromiso

. Personalización

. Confianza

. Eficiencia

Artículo 7 de la constitución política mexicana

Elegí este tema porque el Artículo 7 de nuestra Constitución habla sobre la libertad de difundir opiniones, información e ideas a través de cualquier medio, lo cual hoy en día está totalmente ligado a internet y a las telecomunicaciones. Muchas veces pensamos que las leyes solo aplican para los periodistas o los medios impresos tradicionales, pero en la era digital, la infraestructura de red que nosotros instalamos y administramos es precisamente el canal físico por donde viaja toda esa información. Para mí, como estudiante de informática, conocer este artículo es clave porque me permite entender el marco legal que protege el flujo de datos y la libre expresión en las plataformas digitales, asegurando que los servicios de conectividad que diseñemos respeten y garanticen este derecho fundamental.

El Artículo 7 de la Constitución Política de los Estados Unidos Mexicanos establece que es inviolable la libertad de difundir opiniones, información e ideas, a través de cualquier medio. Esto significa que ninguna ley ni autoridad puede establecer la censura previa, ni coartar la libertad de expresión. En el contexto técnico e informático actual, los puntos más relevantes de este artículo se pueden desglosar en los siguientes aspectos estructurales:

- Inviolabilidad de los medios de difusión: El texto constitucional prohíbe

explícitamente el secuestro o la restricción de los instrumentos utilizados para la difusión de información, lo que en el entorno moderno se traduce en que no se pueden clausurar servidores, bloquear páginas web de manera arbitraria ni confiscar infraestructura tecnológica de telecomunicaciones que sirva para transmitir datos públicos.

- Limitantes claras del derecho: Aunque la libertad es muy amplia, el mismo artículo señala que esta tiene límites legales bien definidos. La difusión de información no debe atacar la moral, la vida privada de las personas, los derechos de terceros, provocar algún delito o perturbar el orden público. Por lo tanto, la libertad de transmisión no exime de responsabilidades legales si se cometen ilícitos digitales.

- Obligación de neutralidad y acceso: El estado no puede restringir el acceso a los medios electrónicos ni tecnológicos. Esto se conecta de forma directa con el principio de neutralidad de la red, garantizando que el tráfico de información e ideas sea libre y equitativo, sin que los proveedores de infraestructura o soporte puedan discriminar o bloquear contenidos según conveniencias particulares.

Llevar el control de la red para una cadena del tamaño de Soriana implica manejar datos masivos de empleados, clientes y proveedores. Aplicar los principios del Artículo 7 constituyente en nuestro servicio operativo diario requiere establecer políticas técnicas muy específicas:

- Implementación de filtros de seguridad justificados: En las redes empresariales de las sucursales de Soriana, configuraremos firewalls y listas de control de acceso (ACL) para bloquear sitios maliciosos o de ocio que afecten la productividad laboral. Sin embargo, nos aseguraríamos de que estas restricciones no violen la libertad de los colaboradores para acceder a herramientas legítimas de información, basándonos estrictamente en la seguridad informática corporativa y no en la censura arbitraria de

ideas.

• Garantía de canales de comunicación internos libres y seguros: Diseñaríamos y daríamos soporte a una arquitectura de red que permita el libre flujo de reportes, opiniones y retroalimentación entre el personal directivo y los empleados de las tiendas Soriana. Al asegurar que los canales digitales sean estables, confidenciales y auditables, fomentamos un entorno de expresión transparente alineado con los derechos constitucionales.

• Protección y blindaje de la infraestructura de transmisión: Al dar mantenimiento a los servidores y nodos locales de Soriana, aplicaríamos protocolos avanzados de cifrado y ciberseguridad. Esto evita que terceros malintencionados ataquen, tumben o intervengan de forma ilegal los sistemas de comunicación de la empresa, salvaguardando la continuidad operativa del negocio y la integridad de los mensajes que viajan por nuestras redes.

La vinculación entre estos tres elementos es directa y complementaria. Mi carrera en Informática me dota de las bases técnicas indispensables para comprender cómo viaja la información digital, cómo auditar el tráfico de datos y cómo implementar esquemas de ciberseguridad. Mi empresa de Redes toma este conocimiento técnico y lo ejecuta operativamente en el mundo real, instalando y asegurando la conectividad de un cliente masivo como Soriana. Finalmente, el Artículo 7 constituye el marco normativo y ético que rige toda esta actividad: nos recuerda que los cables, routers y servidores que desplegamos no son solo fierros, sino autopistas digitales protegidas por la ley para garantizar el derecho humano fundamental de la libre difusión de información.

A manera de conclusión, considero que el Artículo 7 constitucional representa una pauta de alta responsabilidad ética para nuestro ejercicio profesional. Como informáticos y administradores de redes, poseemos el control técnico sobre los accesos y privilegios

de conectividad de miles de usuarios. Utilizar ese poder de manera honesta implica diseñar redes seguras que protejan al negocio sin caer en prácticas abusivas de espionaje o censura injustificada hacia los trabajadores. Al prestarle servicios a una corporación tan importante como Soriana, demostrar que nuestra empresa opera bajo el estricto respeto a las garantías constitucionales y legales eleva nuestro prestigio, asegurando un entorno digital democrático, íntegro y profesional.

Articulo 16 de la constitución política mexicana relativo a la libertad de expresión

Elegí este tema porque hoy en día la tecnología avanza mucho y compartimos mucha información, pero es fundamental saber cuáles son nuestros límites y qué nos protege. El Artículo 16 es la base legal que garantiza que nadie pueda invadir nuestra vida privada, nuestros datos o nuestras pertenencias sin una razón válida y autorizada. En un mundo donde la información es muy valiosa, este artículo actúa como protección frente a abusos, tanto de autoridades como de otras personas. Como estudiante y futuro profesional en tecnología, es necesario conocer este derecho para aplicarlo, respetarlo y defenderlo, tanto en mi vida personal como en mi trabajo. No basta con saber usar herramientas digitales; hay que saber bajo qué reglas deben funcionar para no afectar los derechos de los demás.

El Artículo 16 establece claramente: “Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento”. Esto significa que tenemos derecho a la tranquilidad y a que nadie entre a nuestro espacio, revise nuestras cosas o nos vigile sin permiso ni justificación legal. Se basa en tres reglas importantes: debe haber una ley que lo permita, debe hacerlo una autoridad facultada y siempre debe explicarse por qué se hace. Es nuestra principal protección contra acciones injustas y arbitrarias.

Su protección cubre aspectos esenciales: nuestra persona y familia, resguardando la intimidad, vida personal, relaciones y datos sensibles como salud, creencias o preferencias, evitando que sean revelados sin consentimiento; el domicilio, ya que nuestra casa, oficina o lugar de residencia es inviolable y nadie puede entrar sin permiso o sin una orden judicial autorizada; los papeles y posesiones, que incluyen todo

lo físico y también lo digital como archivos, fotos, correos o información en celulares o nubes, teniendo todo la misma protección legal que un documento en papel; las comunicaciones, asegurando que lo que hablamos o escribimos de forma privada no pueda ser leído, escuchado ni interceptado, salvo casos muy graves y siempre bajo control judicial; y los datos personales, reconociendo nuestro derecho a saber qué información tienen sobre nosotros, además de pedir que se corrija, se borre o se deje de usar.

Al manejar redes e información en mi empresa, aplicaría este artículo como regla principal de operación. Me encargaría de cuidar la información, guardando los datos de clientes y empleados con seguridad mediante sistemas protegidos para que nadie ajeno pueda acceder, modificarlos o difundirlos, cumpliendo también con la ley de protección de datos personales. Establecería políticas claras, definiendo reglas para que solo personal autorizado acceda a la información estrictamente necesaria para su trabajo, e informando siempre a las personas para qué se usan sus datos y por cuánto tiempo se guardan. Implementaría seguridad técnica usando contraseñas seguras, cifrado y herramientas de protección para asegurar que todo viaje y se almacene de forma privada, tal como lo exige la ley, revisando periódicamente que no haya fallos. Respetaría los derechos de las personas, pidiendo siempre permiso antes de recopilar datos y atendiendo rápidamente si alguien pide borrar o corregir su información. Además, contaría con protocolos claros ante autoridades, entregando información solo si recibo una orden escrita, fundada y motivada, verificando que cumpla con todos los requisitos legales.

Este tema me enseña que la tecnología no está por encima de la ley. Para mi carrera profesional, me permite diseñar y administrar sistemas que sean seguros y legales desde su creación, evitando cometer errores que traigan multas, demandas o problemas legales graves. Me convierte en un profesional más completo, que conoce tanto de

redes como de derechos y normativas, lo cual me da ventaja y credibilidad ante clientes importantes. También entiendo que respetar la privacidad genera confianza, y la confianza es lo más valioso para que un negocio crezca y sea estable.

El Artículo 16 es el pilar que protege nuestra libertad e intimidad, y hoy es más importante que nunca ante el uso constante de tecnología. Conocerlo y aplicarlo no es solo una obligación, sino una necesidad para trabajar de forma correcta y segura. Para mi empresa, es la base para operar con ética, evitar riesgos y construir una relación de confianza con los clientes. Entiendo así que la tecnología es una herramienta útil, pero su verdadero valor está en que se use respetando siempre los derechos y límites que la Constitución establece para protegernos.

Articulo 285 Y 576 del Código Penal Federal

Elegí este tema porque estas normas definen conductas delictivas que están directamente relacionadas con la seguridad, la protección de espacios y activos, y la integridad de las personas y organizaciones. Conocer su contenido es fundamental porque establecen límites legales y responsabilidades que deben respetarse en cualquier entorno, y su aplicación es indispensable para prevenir riesgos, evitar sanciones y garantizar el cumplimiento de la ley. Además, estos artículos tienen relación directa con la protección de instalaciones, información y bienes empresariales, por lo que su estudio me permite comprender qué acciones están prohibidas, cuáles son sus consecuencias y cómo diseñar medidas de seguridad que se ajusten a lo que establece la ley. Dominar este conocimiento es necesario para actuar con ética, legalidad y responsabilidad en el ámbito laboral, y para contribuir a que la empresa opere dentro del marco jurídico vigente, protegiendo su patrimonio, su reputación y a todo su personal.

Artículo 285

Se impondrán de un mes a dos años de prisión y multa de diez a cien días de salario, al que, sin motivo justificado, sin orden de autoridad competente y fuera de los casos permitidos por la ley, se introduzca furtivamente, con engaño, violencia o sin permiso de la persona autorizada, a un departamento, vivienda, oficina, recinto o dependencia de cualquier establecimiento, empresa o lugar cerrado o protegido.

Artículo 576

Se sancionará con prisión de cinco a diez años y multa de dieciocho a veinticuatro meses, a quien recabe, facilite, colabore o participe de cualquier forma en actividades, operaciones o fines de bandas armadas, organizaciones o grupos dedicados a acciones ilícitas, delictivas o que atenten contra la seguridad pública, el orden jurídico o los derechos de las personas.

El Artículo 285 protege el derecho a la inviolabilidad de los espacios y recintos, tanto privados como laborales o empresariales. Significa que está prohibido ingresar, permanecer o moverse dentro de instalaciones, oficinas, áreas restringidas o dependencias de la empresa sin contar con autorización expresa, orden legal o causa justificada. Cualquier acceso indebido, aunque no haya robo o daño, ya es un delito y tiene consecuencias penales. Se aplica también a zonas de acceso limitado, archivos, centros de datos, bodegas o áreas donde se resguarda información o bienes, y protege el control que la organización debe tener sobre sus propios espacios.

El Artículo 576 regula y castiga toda participación, apoyo o colaboración con grupos, organizaciones o bandas que actúen fuera de la ley. Significa que cualquier acción que ayude, facilite o forme parte de actividades ilícitas organizadas —ya sea proporcionando información, recursos, acceso, transporte o cualquier tipo de ayuda— es un delito grave con penas mucho más altas. Protege la seguridad colectiva, el orden y la estabilidad, y en el entorno empresarial implica que está prohibido cualquier vínculo, colaboración o

apoyo a grupos que puedan afectar a la empresa, su personal, sus operaciones o su entorno.

En conjunto, significan que la ley protege los recintos y la seguridad, y establece claramente que el acceso indebido y la participación en actividades ilícitas organizadas son conductas penadas, con obligaciones para todos de respetar estos límites y denunciar cualquier riesgo.

Medidas para su cumplimiento

- Reglamentos claros: Elaborar y difundir normas internas que definan quién puede acceder a cada área, cómo se obtienen permisos, qué se considera acceso indebido y las consecuencias de ingresar sin autorización. Se incluye expresamente que violar estas reglas constituye una falta grave y puede ser delito conforme al Artículo 285.

- Control de accesos: Implementar sistemas de identificación, llaves, tarjetas, contraseñas o vigilancia para delimitar y controlar la entrada a oficinas, centros de datos, archivos, bodegas y áreas sensibles. Se registran todos los ingresos y se restringe el paso solo a quienes tienen autorización y necesidad de estar ahí.

- Prevención y prohibición: Establecer reglas estrictas que prohíban cualquier tipo de colaboración, apoyo, contacto o facilitación de información, recursos o acceso a grupos, personas u organizaciones que realicen actividades ilícitas, tal como lo indica el Artículo 576. Se define claramente que cualquier participación en este sentido es inaceptable y conlleva sanciones legales y laborales.

- Capacitación y difusión: Explicar a todo el personal el contenido de ambos artículos, qué conductas están prohibidas, cuáles son sus consecuencias y cómo identificar y reportar situaciones sospechosas. Se enseña que proteger las instalaciones y no colaborar con actividades ilícitas es responsabilidad de todos.

- Protocolos de actuación: Definir qué hacer ante intentos de acceso indebido, personas desconocidas o situaciones que parezcan sospechosas o relacionadas con grupos ilícitos: cómo reportar, a quién acudir y cómo colaborar con autoridades sin poner en riesgo a nadie.

- Supervisión y cumplimiento: Realizar revisiones periódicas de los controles de seguridad, mantener actualizadas las normas y asegurar que se apliquen de forma estricta y uniforme. Registrar y documentar cualquier incidente para tomar medidas y evitar repeticiones.

- Protección de información: Aplicar estas mismas reglas al acceso digital: el ingreso sin permiso a sistemas o datos se considera equivalente y también está prohibido, vinculando estas normas con la seguridad informática y el resguardo de activos.

Ambos artículos son pilares legales de la seguridad y el orden. Definen límites claros sobre lo que es permitido y lo que es delito, protegiendo espacios, personas y bienes. Comprenderlos significa saber qué conductas prevenir, cómo diseñar medidas de protección y cómo asegurar que todas las actividades se mantengan dentro del marco legal. Son normas que aplican siempre, en todo lugar y para todas las personas, y su cumplimiento es obligatorio.

La empresa es un conjunto de espacios, recursos, información y personas, y está protegida directamente por estas normas. El Artículo 285 protege sus instalaciones, oficinas, archivos y zonas operativas contra ingresos indebidos, evitando robos, espionaje, daños o pérdidas. El Artículo 576 protege contra riesgos mayores como la vinculación con grupos ilícitos, lo que podría poner en peligro la continuidad, la reputación y la estabilidad de todo el negocio.

Cumplir con estas leyes permite a la empresa: operar legalmente, evitar sanciones penales o económicas, proteger su patrimonio, generar confianza ante clientes y

autoridades, mantener un entorno seguro para el personal y prevenir riesgos que podrían detener las operaciones. No aplicarlas expone a la organización, a sus directivos y a sus trabajadores a responsabilidades penales y daños irreparables.

Importancia profesional

Este tema es esencial para mi desarrollo profesional, ya que todo trabajo implica respetar la ley, proteger recursos y garantizar seguridad. Conocer y aplicar estos artículos me permite:

- Actuar con responsabilidad y ética, sabiendo identificar conductas prohibidas y evitarlas.
- Diseñar, proponer y supervisar medidas de seguridad y normativas internas que cumplan con la ley, aportando valor y protección a la organización.
- Tomar decisiones informadas y ajustadas al marco jurídico, evitando errores que pudieran generar problemas legales.
- Ser capaz de identificar riesgos, reportarlos y colaborar en su prevención, lo cual es una competencia muy valorada en gestión, seguridad, administración, sistemas y cualquier área operativa.

Este conocimiento fortalece mi perfil, me prepara para asumir mayores responsabilidades y me alinea con el requisito fundamental de todo profesional: trabajar siempre dentro de la ley y proteger los intereses y la seguridad de la organización.

Identificación de delitos y/o faltas administrativas aplicables al usuario.

En el presente reporte se abordarán distintos artículos y normativas legales relacionadas con los derechos de los usuarios dentro de nuestro entorno empresarial,

además de crear conciencia sobre el uso responsable de la información proporcionada a los servicios digitales.

En este documento serán analizados los artículos 6, 7, 8 y 16 de la Constitución Política de los Estados Unidos Mexicanos, los cuales salvaguardan derechos fundamentales como la libertad de expresión, el acceso a la información, el derecho de petición y la privacidad de los datos personales. Asimismo, en conjunto estudiaremos a detalle los artículos 285 y 576 del Código Penal, enfocados en delitos y faltas administrativas vinculadas con el uso indebido de la información y las tecnologías digitales, así como la importancia de la criptografía y su legislación para la protección de datos comprometidos.

Dichos artículos tienen una gran relación con nuestra empresa Hollygather, debido a que informática y la atención con especialistas en el área para garantizar la satisfacción, salvaguardar la integridad y respetar la confidencialidad de nuestros clientes. Por ello, nos resulta fundamental conocer las leyes que regulan el manejo de datos, la seguridad informática y los derechos de cada usuario que forma parte de Hollygather.

Comprender estas normas permite actuar de manera ética y legal dentro del entorno tecnológico, además de fortalecer la protección de la información y prevenir delitos informáticos que puedan afectar tanto a nuestros usuarios como a nuestra empresa

Los artículos 6 y 8 de la Constitución Política de los Estados Unidos Mexicanos forman parte de los derechos fundamentales que protegen a las personas. El artículo 6 establece la libertad de expresión y el derecho a la información, es decir, que cualquier persona puede manifestar sus ideas sin censura previa, siempre y cuando no afecte a terceros, el orden público o constituya algún delito. Por otro lado, el artículo 8 consagra

el derecho

La criptografía y su legislación

tomando como referencia una empresa de tecnología, por ejemplo, una firma dedicada al desarrollo de software, servicios de ciberseguridad, gestión de infraestructuras tecnológicas o soluciones digitales.

Elegí este tema porque, al trabajar en una empresa de tecnología, la criptografía es una herramienta esencial en todos nuestros productos y servicios: la utilizamos para proteger datos de clientes, asegurar comunicaciones, proteger el código de nuestros desarrollos y garantizar la confidencialidad en las transacciones digitales.

Sin embargo, su uso no es libre; está regulado por normas que definen qué prácticas son legales, cuáles constituyen faltas administrativas o delitos y qué responsabilidades debemos asumir. Entender esta normativa es fundamental para evitar sanciones, garantizar que nuestras soluciones cumplan con la ley y ofrecer productos confiables y seguros, aspectos que son clave para la reputación y el funcionamiento de cualquier empresa del sector tecnológico.

La criptografía es el conjunto de técnicas que permiten codificar información para que solo personas o sistemas autorizados puedan acceder a ella, asegurando su confidencialidad, integridad y autenticidad. Desde el punto de vista legal, su regulación

tiene como objetivo equilibrar el derecho a la protección de datos y la privacidad con la necesidad de prevenir y perseguir actividades ilícitas. Sus aspectos principales son:

- Usos permitidos: Está autorizada y fomentada para proteger información sensible, como datos personales, información empresarial, códigos fuente de software, transacciones electrónicas y comunicaciones, cumpliendo así con normativas de protección de datos y seguridad de la información.

- Limitaciones: Se prohíbe su uso para ocultar actividades delictivas, como el robo de información, el fraude, el espionaje o el tráfico ilegal de datos. Además, en muchos países, las empresas deben registrar o notificar el uso de ciertas herramientas criptográficas y,

en caso de requerimiento judicial, deben facilitar el acceso a la información cifrada.

- Delitos y faltas administrativas: El uso indebido —como utilizar algoritmos prohibidos, cifrar información para impedir investigaciones o distribuir herramientas criptográficas sin los permisos correspondientes— puede derivar en sanciones económicas, suspensión de actividades o incluso penas privativas de libertad, dependiendo de la gravedad de la conducta.

- Normativas aplicables: Se rige por leyes generales de protección de datos, leyes específicas de delitos informáticos y normativas sectoriales que regulan el uso de tecnologías, por lo que es necesario conocerlas para adaptar los productos y servicios a los requisitos legales

En mi empresa, lo pondré en práctica de la siguiente manera:

1. Diseño de soluciones legales y seguras: Al desarrollar software o brindar servicios tecnológicos, seleccionaré e implementaré herramientas y algoritmos criptográficos que estén autorizados y reconocidos por la normativa vigente, evitando aquellos que no cumplan con los requisitos legales o que puedan generar riesgos.

2. Políticas internas: Elaboraré y difundiré políticas claras sobre el uso de la criptografía dentro de la empresa, indicando en qué casos se puede utilizar, qué información se debe cifrar y qué procedimientos seguir para cumplir con las obligaciones legales, como la entrega de información cifrada a las autoridades cuando corresponda.

3. Cumplimiento normativo: Verificaré que todos los productos y servicios cumplan con

las leyes locales e internacionales, especialmente cuando se ofrecen soluciones a clientes de distintos países, ya que las regulaciones pueden variar. También me encargaré de mantener los registros y permisos necesarios para el uso de estas tecnologías.

4. Capacitación: Organizaré sesiones de formación para el equipo de trabajo, con el fin de que todos conozcan las normas legales asociadas a esta tecnología, evitando usos indebidos o prácticas que puedan derivar en sanciones o responsabilidades legales.

La Relación que tiene el tema, con mi empresa y mi carrera

Para una empresa de tecnología, el conocimiento de esta normativa es un factor clave de competitividad y confianza. Nos permite ofrecer productos y servicios que cumplen con la ley, lo que aumenta la confianza de los clientes y nos abre la puerta a nuevos mercados. Además, evita riesgos económicos y legales derivados de sanciones o demandas por incumplimiento, protegiendo así el patrimonio y la reputación de la organización.

Como profesional del área tecnológica, este conocimiento me permite desempeñarme con responsabilidad técnica y legal. Podré diseñar soluciones que no solo sean seguras y eficientes, sino también ajustadas al marco normativo, lo que me convierte en un recurso valioso para la empresa. Asimismo, me permite tomar decisiones informadas, asesorar a la organización sobre riesgos y obligaciones, y desarrollar una carrera sólida y confiable en el sector tecnológico

Los Aspectos adicionales relevantes que influyen en nuestra empresa hollygather es

tener en cuenta que la legislación de la criptografía evoluciona constantemente al ritmo de los avances tecnológicos, por lo que es necesario mantenerse actualizado sobre los cambios normativos. Además, en el ámbito tecnológico, el uso adecuado de esta

herramienta no solo es una obligación legal, sino también una ventaja competitiva, ya que los clientes valoran cada vez más la seguridad y el cumplimiento normativo en los productos y servicios que contratan. Por último, el conocimiento de esta normativa ayuda a equilibrar la innovación tecnológica con el respeto a los derechos y obligaciones establecidos por la ley.

La Firma Electrónica y su Legislación

En el presente reporte abordaremos la importancia, fundamentos técnicos y marco legal de la firma electrónica, herramienta esencial para la validez jurídica de las transacciones digitales, así como su aplicación, derechos y obligaciones que implica su uso, vinculándolo con la seguridad jurídica, protección de datos y las buenas prácticas en la gestión de tecnologías de la información.

El tema de la firma electrónica y su legislación se enmarca dentro de la regulación del comercio electrónico y los derechos digitales, y se relaciona con normativas como la Ley de Firma Electrónica Avanzada, el Código Federal de Procedimientos Civiles, la Ley Federal de Protección de Datos Personales y disposiciones del Código Penal Federal.

Estas reglas definen la equivalencia legal con la firma autógrafa, los requisitos de validez, la responsabilidad de los usuarios y la protección de la información que se maneja. También se vincula con conceptos técnicos como la criptografía, certificados digitales y entidades certificadoras, elementos clave para garantizar autenticidad, integridad y no repudio en los actos jurídicos.

Para nuestra empresa HOLLYGATHER, dedicada a redes informáticas, soporte y soluciones tecnológicas, el conocimiento y aplicación de la firma electrónica son fundamentales. Al desarrollar plataformas, gestionar información o prestar servicios, debemos entender cómo funciona legal y técnicamente esta herramienta, qué valor tiene ante la ley y qué requisitos se deben cumplir para su uso seguro.

Esto nos permite: ofrecer soluciones confiables, reducir riesgos legales, agilizar procesos administrativos, cumplir con compromisos formales con nuestros clientes y proteger la información que se maneja. Entender este tema nos ayuda a actuar con seguridad, cumplir la ley y ofrecer confianza a quienes trabajan con nosotros.

Comprender estas normas y principios nos permite evitar nulidades jurídicas, gestionar mejor la identidad digital y garantizar que cualquier documento o trámite electrónico tenga el mismo valor y seguridad que uno físico. Es la base técnica de la firma electrónica: sistema matemático que utiliza dos claves relacionadas: una privada (secreta, solo del titular, sirve para firmar o cifrar) y una pública (abierta, sirve para verificar o descifrar).

Lo que se procesa con una clave solo se resuelve con la otra; garantiza que solo el dueño pudo firmar y que cualquiera puede comprobarlo sin revelar secretos. Es el fundamento sin el cual no existiría seguridad ni validez: sin entender cómo funciona la clave privada y pública, no se comprende por qué la firma es confiable ni cómo se protege la identidad. Es el punto de partida técnico indispensable Funciona como un candado y su llave: la clave privada es la llave que solo tú tienes para cerrar/firmar; la pública es el candado que cualquiera puede usar para verificar que tú lo cerraste. Garantiza tres cosas: autenticidad (sabemos quién fue), integridad (nada cambió) y no repudio (nadie puede negar que lo hizo).

Es invisible, pero es lo que da seguridad matemática. Al diseñar o configurar sistemas, implementaremos protocolos que usen este tipo de criptografía para proteger comunicaciones, accesos y documentos. Explicaremos a nuestros clientes por qué usamos esta tecnología y cómo proteger su clave privada es proteger su identidad legal.

- Empresa: Nos permite desarrollar servicios seguros, diferenciarnos por calidad y cumplir requisitos de ley en seguridad.

- Carrera: Se conecta con seguridad informática, redes y normatividad; es conocimiento técnico esencial para cualquier profesional en tecnologías.

Tiene mismo valor legal que la firma de puño y letra. Ventajas principales: validez jurídica oficial, seguridad absoluta (evita alteraciones o falsificaciones), ahorro (sin

papel ni traslados), rapidez (trámites en segundos), acceso remoto (desde cualquier lugar) y eficiencia en procesos administrativos.

Porque transforma la forma de trabajar: une tecnología con derecho. Conocer sus ventajas es necesario para justificar su uso, modernizar procesos y explicar a clientes y usuarios por qué es mejor y más seguro que lo tradicional Ya no se necesita papel ni presencia física. Cualquier contrato, autorización o trámite f irmado electrónicamente es válido ante autoridades, jueces y terceros. Además, al estar cifrada, es casi imposible de falsificar o alterar. Reduce tiempos, costos y errores, y permite operar 24/7.

Lo implementaremos en contratos con clientes, aceptación de servicios, autorizaciones técnicas y entrega de proyectos. Agilizará nuestra operación y daremos certeza legal a cada acuerdo que firmemos o gestionemos.

- Empresa: Nos hace más competitivos, eficientes y confiables; es una ventaja comercial y legal.

- Carrera: Se vincula con gestión de proyectos, derecho informático y atención al cliente; une lo técnico con lo administrativo.

Es el documento electrónico oficial emitido por una autoridad certificadora autorizada, que vincula tu identidad real con tu clave pública. Contiene tus datos, vigencia y la firma de la autoridad; funciona como tu identificación oficial en internet y es obligatorio para que la firma tenga validez legal.

Porque es el puente entre la tecnología y la ley. Sin él, la firma es solo un código; con él, se convierte en un documento legal. Es necesario saber qué es, quién lo emite y cómo funciona para usarlo correctamente. Lo emiten entidades autorizadas (como el SAT en México). Contiene: nombre, RFC, clave pública, fecha de vigencia y firma de la entidad emisora. Sirve para que cualquiera pueda confiar que esa clave pública sí te pertenece.

Vence y debe renovarse; si se revoca o vence, la firma deja de ser válida.

Gestionaremos nuestros certificados corporativos y asesoraremos a nuestros clientes para que obtengan los suyos de entidades oficiales. Integraremos su uso en nuestros sistemas para que todo trámite quede respaldado legalmente.

- Empresa: Nos da reconocimiento oficial, permitiéndonos operar ante instituciones y generar confianza total.

- Carrera: Se relaciona con legislación informática y gestión de seguridad; es parte de la administración legal de sistemas.

Agencias certificadoras en México Son entidades autorizadas por el Estado para emitir, gestionar y revocar certificados digitales. Principales: SAT (emite la e.firma, la más usada), INE, entidades privadas autorizadas por la Secretaría de Economía y el Poder Judicial. Deben cumplir normas estrictas de seguridad y responsabilidad legal. Porque no cualquiera puede emitir un certificado. Solo las autorizadas por ley dan validez.

Conocerlas es vital para elegir correctamente, evitar fraudes y asegurarse de que todo documento firmado sea aceptado legalmente en México. El SAT es la más importante: su e.firma sirve para todo (fiscal, legal, trámites). Otras entidades solo sirven para usos específicos. Todas están reguladas, deben garantizar seguridad y responden legalmente si cometen errores.

Elegir una no autorizada hace que la firma no valga nada. Trabajaremos exclusivamente con agencias reconocidas oficialmente. En nuestros manuales y servicios, recomendaremos solo estas entidades y explicaremos por qué es riesgoso usar otras.

- Empresa: Nos asegura que nuestros procesos cumplen con la ley, evitando nulidades o problemas legales graves.

- Carrera: Conecta normatividad con administración de servicios; aprendes a gestionar

relaciones con organismos reguladores.

En México, el marco principal es: Ley de Firma Electrónica Avanzada, Código Federal de Procedimientos Civiles, Ley Federal de Protección de Datos Personales y Código Penal Federal.

Establecen validez, usos permitidos, obligaciones, protección de información y sanciones para quien falsifique o use mal estas herramientas. Porque la tecnología tiene reglas. Conocer la ley es obligatorio para saber qué se puede hacer, qué derechos tenemos, qué obligaciones tenemos y qué delitos se cometen si se usa mal. Es la base para no cometer errores.

La Ley de Firma Electrónica Avanzada dice que vale igual que la de puño y letra. El Código Penal Federal castiga con cárcel a quien falsifique, robe o use indebidamente f irmas o certificados. La ley de datos protege la información que contienen. Todo está regulado para dar seguridad jurídica.

Diseñaremos todos nuestros servicios respetando estas leyes: políticas claras, avisos de privacidad, términos de uso y protocolos de seguridad. Capacitaremos al equipo para saber qué es delito y qué es obligación.

- Empresa: Es la protección legal más fuerte; evita demandas, protege datos y da certeza jurídica.

- Carrera: Es el eje de la materia de Normatividad Informática; un profesional debe saber que todo uso tiene consecuencias legales.

En el entorno tecnológico, la firma electrónica aplica a contratos, autorizaciones, informes, trámites ante autoridades y cualquier documento que requiera validez legal. En HOLLYGATHER, esto se traduce en:

- Usar solo certificados de entidades autorizadas.

- Garantizar que nuestros sistemas cumplan requisitos de integridad y seguridad.

- Asesorar a clientes sobre obligaciones y cuidados.

- Cumplir con leyes de protección de datos al manejar información firmada.

- Conocer sanciones y delitos para evitarlos.

Esto demuestra que la tecnología no es solo técnica, sino que tiene un marco jurídico estricto que debemos dominar. Elegimos este tema porque la firma electrónica es la herramienta que hace posible la legalidad total en el mundo digital. Conocer cómo funciona, qué la respalda y qué reglas la rigen nos permite ofrecer servicios modernos, seguros y válidos.

Sin este conocimiento, cualquier trámite o sistema que hagamos podría ser nulo o ilegal. Además, está directamente relacionado con seguridad informática, protección de datos y derechos digitales, temas centrales en nuestra actividad profesional. En los servicios que ofrecemos, dominar este tema nos ayuda a ser más confiables, reducir riesgos legales y mantenernos actualizados en las normas que rigen la tecnología.

- Se vincula con seguridad informática: implementar criptografía y proteger identidades.

- Se conecta con normatividad: conocer leyes, validez y delitos.

- Se relaciona con gestión de servicios: ofrecer soluciones que cumplan requisitos oficiales.

- Se une con ética profesional: saber que manejamos herramientas con valor legal y responsabilidad.

Desde el punto de vista académico, este tema forma parte de materias como normatividad informática, seguridad en redes, legislación informática y ética

profesional. Esto demuestra que trabajar con tecnologías requiere no solo conocimientos técnicos, sino también dominio de las leyes que dan validez y seguridad a todo lo que hacemos.

Código penal federal Artículo 211 bis 1 y 3

Nuestra empresa escogió el tema bis 1 y bis 3 ya que nos habla de fracciones del Código Penal Federal mexicano, junto con el Capítulo I del Título Segundo de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares donde establecen delitos y faltas administrativas que protegen la información de los usuarios.

Y yendo más a fondo sobre estos temas en el Artículo 211 bis 1 Este delito sanciona a quien, sin autorización, intercepte, use, modifique o destruya información contenida en sistemas de informática o equipos terminales protegidos. En redes, esto ocurre cuando alguien captura paquetes de datos (packet sinfín), altera configuraciones de red sin permiso, o elimina registros de logs. La pena es de 6 meses a 4 años de prisión y multa de 200 a 500 días de salario. Protege la confidencialidad e integridad de los datos en tránsito y en reposo, y en el Artículo 211 bis 3 nos habla de que sanciona la creación, distribución o posesión de malware, virus, troyanos, ransomware o cualquier programa diseñado para dañar sistemas. En una empresa de redes, un empleado que instale software malicioso en los equipos de la red corporativa, o que facilite herramientas de hacking a terceros, incurre en este delito. La pena es de 6 meses a 4 años de prisión y multa de 200 a 500 días de salario. Es fundamental para prevenir la introducción de amenazas en la red.

En nuestra empresa lo implementaríamos con un programa integral de cumplimiento normativo que incluya:

- Control de acceso basado en roles (RBAC): Cada técnico solo accede a los equipos y datos estrictamente necesarios para su función, previniendo el acceso ilícito del Art. 211 bis.

- Cifrado de tráfico y segmentación de red (VLANs): Proteger la información en tránsito

con TLS/IPsec y aislar redes de clientes, administración y servidores, evitando la intercepción no autorizada del Art. 211 bis 1.

- Sistemas de detección de intrusos (IDS/IPS) y monitoreo 24/7: Detectar intentos de acceso no autorizado, malware o anomalías en tiempo real, protegiendo contra el daño del Art. 211 bis 1 y la introducción de programas maliciosos del Art. 211 bis 3

- Auditorías trimestrales de seguridad: Evaluar vulnerabilidades en routers, switches, firewalls y servidores, con reportes de cumplimiento normativo para demostrar debido diligencia ante autoridades.

Estos temas tienen mucha relación con mi carrera y nuestra empresa ya que en nuestra empresa cumplir con estos artículos significa operar con respaldo legal y así evitando sanciones penales y administrativas que pueda afectar a nuestro cliente, y en mi carrera tiene relación ya que esto tiene que ver algo con la informática.

Definición de datos

La definición de datos es un tema fundamental dentro del ámbito tecnológico y empresarial, ya que los datos representan la base sobre la cual se generan procesos, información y toma de decisiones. Los datos son representaciones de hechos, ideas, conceptos o instrucciones que pueden ser almacenados, procesados y utilizados con un propósito específico. Se presentan en diferentes formatos como números, letras, imágenes, sonidos, símbolos o registros digitales.

Actualmente, las empresas dependen de los datos para operar de manera eficiente. Sin ellos sería imposible mantener un control administrativo, financiero y tecnológico adecuado. En una empresa dedicada a redes y conexiones como HollyGather, el uso de datos es permanente debido a la necesidad de administrar servicios de internet, monitorear conexiones y proteger sistemas informáticos.

Los datos, por sí solos, pueden no tener significado completo; sin embargo, cuando se organizan y analizan se convierten en información útil que ayuda a resolver problemas y tomar decisiones estratégicas.

Dentro de HollyGather, los datos pueden encontrarse en:

- Registros de clientes
- Direcciones IP
- Configuraciones de routers y switches
- Contraseñas cifradas
- Historiales de mantenimiento
- Contratos de servicios

- Inventarios de equipos
- Reportes técnicos
- Bitácoras de acceso y monitoreo
- Información de proveedores y socios comerciales

La correcta administración de estos datos permite que HollyGather mantenga estabilidad operativa, rapidez en sus servicios y mejor control de los recursos tecnológicos.

La importancia de los datos también radica en que representan un activo empresarial valioso. La pérdida, alteración o robo de información puede afectar el funcionamiento de la empresa y generar daños económicos o legales.

Datos personales

Los datos personales son toda información relacionada con una persona física que permite identificarla de forma directa o indirecta. Su finalidad principal es registrar, reconocer o mantener comunicación con individuos dentro de procesos empresariales y administrativos.

Algunos datos personales comunes incluyen:

- Nombre completo
- Dirección particular
- Número telefónico
- Correo electrónico
- Fecha y lugar de nacimiento
- Fotografías
- Firma
- CURP o identificación oficial
- Información laboral
- Datos académicos

En HollyGather, los datos personales son indispensables para establecer relaciones comerciales y laborales. Se utilizan para registrar clientes, elaborar contratos, gestionar pagos, brindar soporte técnico y administrar expedientes de empleados.

El manejo incorrecto de estos datos puede generar problemas como:

- Robo de identidad

- Fraudes financieros
- Suplantación de identidad
- Pérdida de confianza del cliente
- Problemas legales

Por esta razón, HollyGather debe implementar medidas de protección como autenticación de usuarios, permisos limitados, políticas de privacidad y sistemas seguros de almacenamiento.

La protección de datos personales también fomenta la confianza entre empresa y cliente, demostrando responsabilidad y profesionalismo.

Datos sensibles

Los datos sensibles son aquellos que contienen información privada o delicada que puede afectar la dignidad, seguridad o privacidad de una persona si se divulga sin autorización.

Estos datos requieren mayor protección debido a que su exposición puede provocar discriminación o daños personales y económicos.

Algunos ejemplos incluyen:

- Información médica
- Historial clínico
- Datos biométricos
- Huellas digitales
- Reconocimiento facial

- Datos financieros y bancarios
- Información patrimonial
- Contraseñas y claves de acceso
- Información privada del trabajador o cliente

En HollyGather, el manejo de datos sensibles es especialmente importante debido al trabajo relacionado con tecnología y seguridad informática.

La empresa debe utilizar:

- Cifrado de información
- Sistemas de autenticación avanzada
- Restricciones de acceso
- Monitoreo continuo
- Protocolos de seguridad

El uso de estas medidas disminuye riesgos relacionados con ataques cibernéticos, filtraciones o accesos indebidos.

Además, los datos sensibles requieren un nivel ético de responsabilidad, ya que su protección no solo es una obligación tecnológica sino también moral y profesional.

Archivo, registro, base o banco de datos

El archivo, registro, base o banco de datos es un sistema organizado diseñado para almacenar y administrar información.

Su función principal es mantener la información ordenada y disponible para facilitar la consulta y actualización.

Las bases de datos pueden clasificarse en:

Bases de datos físicas

Se encuentran en documentos impresos, carpetas o expedientes físicos.

Bases de datos digitales

Se almacenan en computadoras, servidores o plataformas digitales especializadas.

En HollyGather, las bases de datos son esenciales para organizar información como:

- Expedientes de clientes
- Historiales de soporte técnico
- Facturación y pagos
- Contratos de servicio
- Inventarios de equipos
- Información de proveedores
- Registros de mantenimiento
- Reportes de incidencias
- Monitoreo de conexiones

El uso de bases de datos aporta ventajas como:

- Mayor rapidez de búsqueda
- Reducción de errores
- Mejor control administrativo
- Optimización de recursos

- Protección y respaldo de información
- Mejor atención al cliente

Las bases de datos también ayudan a realizar análisis y reportes que apoyan la planeación y crecimiento empresarial.

Tratamiento de datos

El tratamiento de datos comprende todas las actividades y operaciones realizadas con la información desde que es recopilada hasta su eliminación definitiva.

Este proceso es fundamental porque garantiza el uso responsable y seguro de la información.

Las etapas del tratamiento de datos incluyen:

- Recolección
- Registro
- Organización
- Clasificación
- Almacenamiento
- Consulta
- Actualización
- Modificación
- Transferencia
- Respaldo
- Eliminación

En HollyGather, el tratamiento de datos debe desarrollarse siguiendo normas internas y protocolos de seguridad informática.

Para ello se utilizan herramientas y prácticas como:

- Firewalls
- Antivirus
- Copias de seguridad
- Cifrado de archivos
- Monitoreo de accesos
- Auditorías digitales
- Políticas de privacidad
- Capacitación constante del personal

El tratamiento responsable de datos permite prevenir:

- Pérdida de información
- Ataques cibernéticos
- Robo de datos
- Alteración de registros
- Accesos no autorizados

Un manejo adecuado de la información mejora la continuidad operativa y fortalece la imagen profesional de la empresa.

Aplicación en HollyGather

En HollyGather, la aplicación de estos principios es necesaria para garantizar seguridad

y eficiencia en los servicios de redes y conexiones.

La empresa implementa controles tecnológicos y administrativos destinados a proteger la información.

Entre las medidas utilizadas se encuentran:

- Contraseñas seguras
- Firewalls empresariales
- Antivirus actualizados
- Monitoreo de tráfico de red
- Respaldos automáticos
- Restricción de accesos
- Cifrado de datos
- Auditorías de seguridad
- Capacitación del personal

Estas acciones permiten mantener la confidencialidad, disponibilidad e integridad de los datos.

El cumplimiento de estas prácticas mejora la confianza de los clientes y fortalece la reputación empresarial.

Relación con HollyGather y la carrera

La relación entre este tema, HollyGather y la carrera es directa debido a que las empresas tecnológicas dependen del manejo y protección de información digital.

La carrera de informática, redes y telecomunicaciones exige conocimientos sobre:

- Seguridad informática
- Administración de bases de datos
- Protección de información
- Configuración de redes
- Prevención de riesgos digitales

Comprender la definición y tratamiento de datos permite desarrollar habilidades profesionales necesarias para diseñar sistemas seguros y eficientes.

Además, fortalece valores como ética, responsabilidad y confidencialidad, elementos indispensables para el desempeño profesional dentro del área tecnológica y empresarial.

Implicados en el daño a datos.

El “daño a datos” se define como la alteración, pérdida o destrucción de información electrónica, lo que afecta su integridad, disponibilidad y confiabilidad. Los implicados suelen ser tanto los atacantes (hackers, incides maliciosos, grupos organizados) como las víctimas (individuos, empresas o instituciones) que sufren las consecuencias de los usuarios por robo de datos de los sistemas operativos q tienen algunas veces los ataques de “DOS” común mente sufren los robo los usuarios de la empresa que lleva acabo los datos relevantes de cada usuario.

El implicado a datos este tema se lleva a cabo en nuestra empresa ya q nuestros, datos pueden tener datos importantes de cada usuario especifico esto nos ayudaría a que nuestros datos no sean robados, en los implicados a datos están (la victima) y el (agresor) ya q nos tomaría los datos

En este tema lo elegimos por los mismos datos de los datos variados, q se llevan a cabo de los q se recopilan los datos de las personas q tienen q confiar en la seguridad de la empresa.

Mayormente se tiene y se lleva acabo el daño a datos “en nuestra carrera se mantiene en una formación de andar configurando los datos de las direcciones ip al igual q la seguridad q se tiene en la empresa el testimonio de los datos …

Al aplicarlo en nuestra empresa se daría a mantener los datos de manera eficiente en donde se configura los datos, y se mantiene un respaldo de los datos, nuestra empresa recopilaría los datos específicos de cada uno e ingresaría direcciones ip y mayor seguridad para cada usuario q tenga una eficiencia buena y no sufra pedida de los datos.

Piratería y Falsificación de software

Elegí este tema porque, la verdad, cuando estás metido en la instalación y el soporte de redes, te das cuenta de que el software no es un accesorio, es lo que hace que todo funcione. Trabajar con sistemas operativos de red, firewalls o programas de gestión que sean piratas o falsificados es una bomba de tiempo. No solo pones en riesgo la estabilidad y los datos de la empresa que te está contratando, sino que te juegas tu propia reputación como profesional. En nuestra carrera de informática, entender el impacto real de usar software sin licencia es fundamental para no meter la pata en proyectos grandes.

Para entenderlo de forma sencilla, la piratería de software es básicamente usar, copiar o distribuir un programa sin pagar la licencia ni tener el permiso del creador. Por otro lado, la falsificación ya es algo más pesado, porque es cuando duplican el producto y te lo venden haciéndolo pasar por el original. En el mundo de las redes y los servidores, esto nos pega directo en tres puntos críticos:

- Riesgos de seguridad brutales: El software alterado o bajado de sitios raros casi siempre viene con sorpresas. Te meten malware, troyanos o puertas traseras (backdoors) sin que te des cuenta, dejando la red abierta para que cualquiera se robe información confidencial.

- Cero actualizaciones y soporte: Un sistema pirata jamás va a recibir los parches de seguridad oficiales del fabricante. Si sale una vulnerabilidad nueva en el mercado, tu red se queda totalmente expuesta porque no hay forma de actualizar el firmware de manera legal.

- Problemas legales y multas: Utilizar programas ilegales en un entorno corporativo es un delito de propiedad intelectual. Si a la empresa le cae una auditoría de software, las

multas económicas son gigantescas y pueden llegar hasta demandas penales que tumban el negocio.

Si mi empresa le va a dar soporte y manejar las redes a un cliente del tamaño de Soriana, la responsabilidad es enorme. Para aplicar este tema en el servicio del día a día, implementaría tres medidas muy claras:

- Auditorías de activos de red: Lo primero sería hacer un escaneo a fondo en toda la infraestructura que les manejamos (routers, switches, servidores) para revisar que cada sistema operativo de red y herramienta de monitoreo tenga sus licencias originales y vigentes.
- Uso estricto de software oficial o libre: Nos aseguraríamos de instalar únicamente software directo de los fabricantes autorizados o, en su defecto, implementar soluciones de código abierto (open-source) que sean estables, legales y seguras para la operación.
- Bloqueo de instalaciones en sucursales: Configuraríamos las directivas de seguridad en los servidores para que ningún usuario o empleado de las tiendas pueda instalar programas por su cuenta. Así evitamos que metan software pirata o aplicaciones crackeadas que infecten la red interna.

Aquí todo se conecta a la perfección. Mi carrera en Informática me da la teoría y los conocimientos técnicos para entender cómo operan las licencias, cómo identificar software malicioso y cómo estructurar sistemas seguros. Por otra parte, mi empresa de Redes es la que lleva ese conocimiento a la práctica en el mundo real, instalando y asegurando que la conectividad de Soriana sea impecable. Y finalmente, el tema de la piratería es el estándar ético y de seguridad que une a ambas: nos recuerda que para ofrecer un servicio profesional y competitivo, todo lo que instalemos debe ser 100% legal y confiable.

Como conclusión, creo que evitar la piratería y la falsificación de software va mucho más allá de cumplir con la ley; es una cuestión de ética y profesionalismo. Cuando trabajas con un cliente grande como Soriana, estás manejando la infraestructura por donde pasa su negocio y la confianza de mucha gente. Usar software original es la única forma real de garantizar que la red no se va a caer por un fallo de seguridad y de demostrar que como informáticos hacemos las cosas bien, con calidad y de manera honesta.

Aplicación del Capítulo IV de la Ley Federal del Derecho de Autor en Hollygather

Como dueño de Hollygather, empresa dedicada a crear, administrar y operar redes de conexión para distribuir contenido, información y materiales diversos a grandes cadenas comerciales como Soriana, tengo claro que el éxito y la estabilidad de mi negocio dependen totalmente de operar bajo el marco legal vigente. El Capítulo IV de la Ley Federal del Derecho de Autor de México, que regula todo lo relativo a la comunicación pública de obras protegidas, es fundamental para mi actividad, ya que todo lo que hacemos: transmitir, entregar o facilitar el acceso a contenido, entra en lo que esta norma regula. En este reporte explico por qué elegí este tema, su contenido, cómo lo aplico en mi empresa y la relación que tiene con mi negocio y mi formación profesional.

Elegí este capítulo porque es la base legal exacta sobre la que funciona Hollygather. Mi negocio consiste en ser el puente entre quienes generan o poseen contenido y empresas que lo necesitan, como Soriana, y todo acto de entregar o transmitir ese material se define legalmente como comunicación pública, actividad que este apartado de la ley regula al detalle. Lo escogí por razones esenciales para mí como dueño: Seguridad jurídica. Si no cumplo con estas reglas, mi empresa corre riesgos graves: multas importantes, demandas por daños, suspensión de operaciones o incluso procesos legales. Al ser proveedor de Soriana, una empresa con altos estándares de cumplimiento, yo debo garantizar que mi servicio no les genere problemas legales a ellos; si fallo en esto, pierdo contratos y reputación.

Es mi forma de trabajar. No solo es una obligación, es mi ventaja competitiva. En el mercado hay muchas empresas que distribuyen contenido sin revisar si es legal. Yo, al conocer y aplicar estas normas, ofrezco algo que otros no: seguridad y confianza. Eso hace que Soriana y otros clientes prefieran trabajar conmigo y me den su confianza a

largo plazo. Sostenibilidad del negocio. Como dueño, mi objetivo es que Hollygather crezca y se mantenga en el tiempo. El respeto a los derechos de autor no es un trámite, sino la regla que me permite operar de forma ética, legal y estable. Sin esto, el negocio no tiene futuro. En resumen, lo elegí porque es el marco que me dice qué puedo hacer, cómo y qué debo cuidar para que mi empresa funcione bien.

El Capítulo IV, titulado De la Comunicación Pública, establece las reglas para usar, difundir o poner al alcance de terceros cualquier obra protegida: literaria, artística, científica, material audiovisual, publicitario o cualquier contenido que sea creación de alguien. Sus puntos clave son: Qué es comunicación pública.

Es cualquier acción en la que una obra se entrega, transmite o se pone a disposición de personas que no son del entorno privado del creador. Para Hollygather, esto significa que cada vez que enviamos contenido a las plataformas o sucursales de Soriana, estamos realizando un acto regulado por esta ley.

No es algo libre, es algo que requiere autorización. Derechos exclusivos. Solo el autor o quien tenga los derechos patrimoniales de la obra puede decidir quién la usa, cómo y por cuánto tiempo. Nadie, incluida mi empresa, puede distribuir, modificar o entregar ese contenido sin tener una autorización por escrito, válida y detallada. Esa autorización debe decir claramente qué se puede hacer y qué no.

Obligaciones del intermediario. Como empresa de redes y distribución, la ley me asigna responsabilidades claras: yo debo verificar que quien me da el contenido tenga derecho a difundirlo, no puedo alterar la obra sin permiso, siempre debo reconocer su origen y solo puedo usarla dentro de lo que se haya pactado. También debo guardar todos los documentos que prueben que todo está legal, por si alguna autoridad o alguien reclama. Límites.

Hay usos permitidos sin autorización, pero son solo para fines educativos o informativos, sin ganar dinero. Como Hollygather es un negocio comercial y trabaja con empresas como Soriana, esas excepciones no aplican para nada; todo lo que distribuimos debe tener su permiso legal. Consecuencias. Si se infringen estas reglas, las sanciones van desde multas altas, hasta tener que pagar indemnizaciones por daños, detener la distribución y, en casos graves, consecuencias penales. En pocas palabras, este capítulo me dice que distribuir contenido es un servicio regulado, y que la única forma de hacerlo bien es respetando los derechos de quien creó ese material.

Como dueño, he diseñado todos los procesos de mi empresa para cumplir estrictamente con estas reglas, especialmente en lo que hacemos para Soriana. Revisión obligatoria: antes de recibir cualquier contenido y antes de subir algo a mis redes, le exijo a quien me lo entrega que me presente las licencias, contratos o autorizaciones completas.

Reviso que esté todo claro: qué contenido es, para qué sirve, por cuánto tiempo y si se puede distribuir a empresas como Soriana. Si falta algún papel o algo no está claro, no lo acepto. Es mi primera regla de seguridad. Contratos claros con Soriana: en los acuerdos que firmo con ellos, incluyo cláusulas específicas sobre derechos de autor.

Detallo exactamente qué contenido les entrego, para qué uso es (por ejemplo, solo para exhibición en tiendas, o solo para difusión interna) y por cuánto tiempo. Dejo claro que Soriana solo puede usarlo, así como lo acordamos; si quieren darle otro uso, tienen que avisarme para gestionar una nueva autorización. Yo me comprometo a entregarles solo material legal, y ellos se comprometen a respetar las condiciones de uso.

Así, ambos estamos protegidos. Controles técnicos y administrativos: tengo configuradas mis redes para que el contenido solo se pueda usar como se pactó; por ejemplo, si es solo para verlo y no para descargar, el sistema bloquea la descarga. Llevo

un registro detallado de todo: qué envié, cuándo, a quién, y qué documentos respaldan su legalidad. Guardo toda esa información por años, como lo marca la ley, para tener pruebas si algo llega a reclamarse.

Capacitación a mi equipo: todo mi personal, desde operaciones hasta atención a clientes, sabe y entiende estas reglas. Les he explicado qué está permitido y qué no, y les he enseñado a revisar que todo esté en orden. Para mí, es vital que todos trabajen con el mismo cuidado legal. Procedimiento ante reclamos: tengo definido qué hacer si alguien reclama que usé algo sin permiso: suspendo la distribución de inmediato, reviso mis registros, hablo con las partes involucradas y resuelvo conforme a la ley, siempre avisando a Soriana para no afectar su operación.

Esta norma es la razón por la que Hollygather existe y funciona. Mi negocio no crea contenido, lo distribuye; por lo tanto, mi valor para clientes como Soriana es entregarles material que ellos puedan usar sin miedo a problemas legales. Sin el Capítulo IV, no sabría cómo operar, y mi servicio no tendría valor ni seguridad. La relación es directa: estas reglas definen mi actividad, mis límites y mis obligaciones. Cumplir con ellas es lo que me permite ser un proveedor confiable, mantener mis contratos y hacer crecer la empresa. Es la base de mi negocio.

Como dueño y profesional, esta norma está totalmente ligada a mi desarrollo y formación. Hago negocios con base en la ley: Conocer este tema me permite tomar decisiones seguras, diseñar procesos correctos y evitar errores que podrían acabar con mi empresa. No soy solo un administrador, soy un empresario que sabe cómo moverse dentro del marco legal. Me da una ventaja profesional: Saber cómo funciona la propiedad intelectual en redes y distribución es un conocimiento que pocos tienen. Esto me hace más competente, me permite negociar mejor con grandes empresas y me

posiciona como un experto en mi ramo. Visión de largo plazo: Entiendo que cumplir la ley no es un gasto, sino una inversión. Esa forma de pensar me ayuda a dirigir Hollygather con estrategia, ética y responsabilidad, cualidades que definen mi perfil como empresario y mi crecimiento profesional.

Acceso no autorización a sistemas de información

Elegí este tema porque en la actualidad la tecnología es parte fundamental de todas las actividades, y los sistemas de información almacenan datos muy valiosos como información de clientes, registros financieros, procesos operativos y secretos empresariales. Me llamó la atención porque es un riesgo constante que puede afectar el funcionamiento, la economía y la reputación de cualquier organización. Además, considero que es un asunto relevante que requiere conocimiento y medidas adecuadas para proteger los recursos, por lo que estudiar y aplicar soluciones en este ámbito es una responsabilidad importante para cualquier persona que trabaje con tecnología o gestión de información.

Se refiere a la acción de ingresar, manipular, copiar o utilizar sistemas de información, redes o dispositivos electrónicos sin contar con la autorización legal o el permiso correspondiente por parte de los dueños o administradores de dichos recursos. Esto incluye actividades como el acceso a cuentas ajenas, la violación de contraseñas, la intrusión en redes privadas, la alteración de datos sin autorización o el uso de herramientas para eludir las medidas de seguridad establecidas.

Significa que existe una violación a las normas de seguridad y a la privacidad de los recursos digitales. No solo se trata de un acto ilegal en la mayoría de los países, sino que representa un riesgo grave: puede provocar pérdidas económicas, fuga de información confidencial, interrupción de operaciones, daño a la imagen de la empresa y vulneración de los derechos de las personas o instituciones involucradas. En términos sencillos, significa que se está accediendo a información o sistemas que no están destinados a ser utilizados por quien lo hace.

Para aplicar medidas contra el acceso no autorizado, implementaría las siguientes

acciones:

- Establecer políticas claras: Definir reglas sobre quién puede acceder a qué información, cómo se deben usar los dispositivos y sistemas, y cuáles son las consecuencias de incumplir estas normas.

- Control de accesos: Asignar permisos de forma selectiva: cada persona solo tendrá acceso a la información que necesita para realizar sus funciones. Usar contraseñas seguras, autenticación de dos pasos y cambiar claves periódicamente.
- Capacitación: Enseñar a todo el personal sobre los riesgos, cómo identificar intentos de intrusión y cuáles son las buenas prácticas para proteger los sistemas.
- Monitoreo y seguimiento: Llevar un registro de los accesos a los sistemas para detectar actividades inusuales o sospechosas de forma oportuna.
- Medidas técnicas: Instalar cortafuegos, programas antivirus y sistemas de detección de intrusiones, además de mantener actualizado el software y los equipos.

El acceso no autorizado es un problema que afecta directamente la estabilidad y el funcionamiento de cualquier organización, por lo que su prevención y control son actividades esenciales.

mi empresa maneja información digital, datos de clientes, registros contables o procesos operativos a través de sistemas electrónicos, está expuesta a este riesgo. Aplicar las medidas mencionadas no solo protege los recursos de la empresa, sino que también garantiza que las operaciones se realicen sin interrupciones, se cumplan las normativas legales y se mantenga la confianza de los clientes y socios.

Si mi carrera está relacionada con la tecnología, la administración, la gestión de

sistemas o la seguridad informática, este tema es fundamental porque:

- Me permite adquirir conocimientos para desempeñar mi trabajo de forma más responsable y eficiente.
- Me permite aportar soluciones útiles para la organización donde trabajo.
- Me ayuda a cumplir con las responsabilidades éticas y legales que corresponden a mi profesión.
- Me prepara para identificar riesgos y proponer mejoras que aporten valor y seguridad al entorno laboral.

Este tema une lo que dice la ley con lo que hago todos los días, y es lo que me permite tener un negocio sólido, confiable y exitoso como Hollygather.

Autoría y creación de software

La autoría de software se refiere a la titularidad de los derechos morales y patrimoniales sobre un programa de cómputo. En México, estos derechos están reconocidos y protegidos por la Ley Federal del Derecho de Autor (LFDA), específicamente en sus artículos 13, 101, 102 y 111, así como por el Código Penal Federal en sus artículos 424 Bis y 424 Ter.

En Hollygather, todo software, aplicación, script, base de datos o herramienta tecnológica desarrollada por el personal durante su jornada laboral, utilizando equipos, licencias, tiempo o recursos propiedad de la empresa, se considera obra por encargo conforme al artículo 83 de la LFDA. Por lo tanto, los derechos patrimoniales de explotación, reproducción, distribución y modificación pertenecen exclusivamente a Hollygather, respetando en todo momento los derechos morales del autor, como el reconocimiento de su nombre y la integridad de la obra.

El proceso de creación de software en Hollygather se rige bajo las siguientes políticas institucionales:

Todo código fuente generado debe documentarse obligatoriamente en los repositorios oficiales de Hollygather, indicando: nombre completo del autor, fecha de creación, versión, descripción funcional y dependencias utilizadas. Esto garantiza la trazabilidad y protege los derechos de autor.

Propiedad intelectual y confidencialidad:

El software desarrollado constituye un activo intangible de Hollygather. Queda estrictamente prohibida su reproducción, distribución, venta o modificación sin autorización por escrito del área jurídica y de TI. El colaborador firma un acuerdo de confidencialidad al recibir bienes informáticos.

Licenciamiento y software de terceros:

Hollygather respeta los derechos de autor de terceros. Por ello, se prohíbe instalar, ejecutar o distribuir programas sin licencia válida en los equipos asignados. El área de TI realizará auditorías periódicas para verificar el cumplimiento. El uso de software libre debe ser aprobado previamente y cumplir con sus términos de licencia.

Responsabilidad legal y sanciones:

El mal uso, plagio, sustracción o distribución no autorizada de software constituye una falta administrativa grave. De acuerdo con los artículos 424 Bis y 424 Ter del Código Penal Federal, la reproducción no autorizada de programas de cómputo se sanciona con prisión de 6 meses a 6 años y multa de 300 a 3,000 días de salario mínimo. A nivel interno, puede resultar en la rescisión de contrato sin responsabilidad para Hollygather.

Uso de Inteligencia Artificial en el desarrollo:

Si se utilizan herramientas de IA para generar código, el colaborador debe revisar y validar que no infrinja derechos de autor de terceros. El producto final será propiedad de Hollygather bajo los mismos términos.

Relación con la Asignación de Bienes Informáticos:

Al recibir un equipo de cómputo, el usuario acepta estas políticas mediante la carta responsiva. El equipo es una herramienta de trabajo, por lo que todo producto intelectual generado con él durante el horario laboral pertenece a Hollygather. Esto evita conflictos legales y protege la inversión tecnológica de la empresa.

Estas medidas garantizan la protección de los activos digitales de Hollygather, aseguran el cumplimiento del marco legal mexicano y fomentan una cultura de desarrollo ético, seguro y responsable de soluciones tecnológicas.

Asignación de bienes informáticos

En el presente reporte abordaremos distintos artículos y normativas legales relacionadas con los derechos de usuarios dentro de nuestro entorno empresarial, además de hacer Determinación de los lineamientos para la utilización de recursos tecnológicos en el ámbito organizacional.

Las organizaciones deben establecer políticas claras que regulen el uso de sus equipos de cómputo. En Hollygather, la asignación de bienes informáticos se realiza bajo lineamientos específicos que definen las responsabilidades del usuario, los usos permitidos y las restricciones aplicables, con el fin de proteger la información y garantizar el cumplimiento del marco legal vigente.

La identificación de políticas y controles aplicables al software y sistemas de una organización es fundamental para garantizar la operación segura y legal de la infraestructura tecnológica. En Hollygather, estos lineamientos regulan desde la instalación de programas hasta la protección de los datos críticos de la empresa y sus clientes.

- Uso de software autorizado: Solo se permite la instalación de programas con licencia válida y aprobados por el área de TI. Queda estrictamente prohibido el uso de software pirata o no autorizado en los equipos asignados, ya que infringe la Ley Federal del Derecho de Autor y expone a Hollygather a sanciones legales.

- Actualizaciones y parches: Todos los sistemas operativos y aplicaciones deben mantenerse actualizados para corregir vulnerabilidades. El área de TI programa actualizaciones automáticas fuera del horario laboral para no afectar la productividad.

- Control de acceso: El acceso a sistemas críticos se gestiona mediante usuarios y contraseñas únicos, autenticación de dos factores y permisos basados en roles. Ningún colaborador debe compartir sus credenciales.

- Monitoreo y auditorías: Se realizan revisiones periódicas de los sistemas para detectar accesos no autorizados, software malicioso o incumplimiento de políticas. Se utilizan firewalls, antivirus empresariales y sistemas de detección de intrusos.

- Segregación de funciones: El personal de desarrollo no tiene acceso a los servidores de producción, y el personal de soporte no puede modificar código fuente. Esto reduce riesgos de errores y fraudes internos.

- Registro de actividades: Todos los accesos a sistemas con información sensible quedan registrados en bitácoras para auditoría y trazabilidad.

Respaldos de información en Hollygather:

La pérdida de datos puede representar daños económicos y legales graves para la empresa. Por ello, en Hollygather se implementa la política de respaldos 3-2-1:

Regla Aplicación en Hollygather

3 copias de los datos Original + 2 respaldos

2 tipos de medios diferentes Servidor local + nube

Frecuencia de respaldos:

información crítica: Respaldos diarios automatizados a las 11:00 pm.

Bases de datos de clientes: Respaldos cada 4 horas.

Equipos de usuarios: Respaldos semanales de carpetas institucionales.

Al recibir un equipo de Hollygather, el colaborador se compromete a guardar toda la información laboral en las carpetas de red asignadas, ya que solo esas carpetas están incluidas en el protocolo de respaldo. La información almacenada en el escritorio o en discos locales no está protegida y su pérdida será responsabilidad del usuario.

El incumplimiento de estas políticas y controles constituye una falta administrativa y puede derivar en sanciones internas, rescisión de contrato o acciones legales conforme al Código Penal Federal, artículos 211 Bis y 424 Ter, relacionados con delitos informáticos.

Estas medidas permiten que Hollygather garantice la integridad, confidencialidad y disponibilidad de la información, cumpla con normativas como la Ley Federal de Protección de Datos Personales y mantenga la confianza de sus clientes.

Normativas aplicadas en el equipo de computo

Es fundamental la garantía de la seguridad de los datos, y la eficiencia operativa y el cumplimiento legal dentro de cualquier infraestructura tecnológica. además, nos permitiría entender como protegemos los activos frente a las vulnerabilidades y estandarización de nuestros equipos de cómputo en tener el proceso de algún mantenimiento e/y algún soporte técnico

Nuestro desarrollo en equipo de cómputo garantiza la seguridad, eficiencia y sostenibilidad de nuestra empresa para mantener una seguridad de nuestros datos confidenciales, también es necesario tener algún soporte técnico q nos ayude a garantizar la seguridad de los equipos de cómputo.

En nuestra empresa de trata de mantener algunas normatividades en nuestros equipos para q no sufran alguna vulnerabilidad. Nuestra empresa se aria algunas áreas q se tienen que mantener estables a cualquier riesgo que tenga que ver con los datos de las personas asociadas que estén con nosotros en cualquier proyecto etc.

Como los implementaríamos nuestra empresa

Esto en mi empresa lo implementaríamos manteniendo un acceso solamente registrado para nuestros equipos al igual que mantendríamos algún soporte de antivirus que nos ayudaría a mantener asegurado de cualquier riesgo alguno sobre robo de datos personales de algún cliente o algún compañero de trabajo.

Pues Relación en carrera y empresa

Pues en cuestión de nuestra carrera e/y empresa se basaría q en nuestra carrera de informática nos da las herramientas necesarias para cualquier manipulación de los datos

necesarios para proteger datos y también la codificación de algoritmos para controlar datos y en nuestra empresa sería lo mismo nomas q con la diferencia seria mantener seguro los datos de nuestros clientes.

Acceso No Autorizado en Equipos de Cómputo y Telecomunicaciones

El acceso no autorizado en equipos de cómputo y telecomunicaciones es un tema de gran relevancia debido al crecimiento del uso de la tecnología en todos los sectores productivos y comerciales. En la actualidad, las empresas almacenan gran cantidad de información en computadoras, servidores y plataformas digitales, convirtiendo los sistemas tecnológicos en herramientas indispensables para el funcionamiento diario.

El desarrollo de internet, la conectividad y la digitalización de procesos ha permitido mejorar la productividad y la comunicación empresarial; sin embargo, también ha aumentado la exposición a amenazas informáticas. Muchas organizaciones enfrentan problemas relacionados con robo de información, espionaje digital, alteración de archivos y ataques a redes.

Por esta razón, este tema fue elegido para analizar la importancia de proteger los equipos y sistemas de telecomunicaciones frente a accesos ilegales que ponen en riesgo la seguridad y estabilidad de las empresas.

Para HollyGather, empresa dedicada a redes, conexiones y mantenimiento tecnológico, el estudio de este tema es esencial porque sus actividades dependen directamente del funcionamiento seguro de redes y equipos de comunicación. La empresa trabaja con organizaciones comerciales y distribuidoras que requieren protección de datos y continuidad en sus operaciones.

Además, conocer este tema permite desarrollar responsabilidad profesional y ética en el

manejo de información digital, fortaleciendo la preparación académica y laboral dentro del área de informática y telecomunicaciones.

El acceso no autorizado se define como la entrada, manipulación o permanencia en equipos de cómputo, sistemas informáticos o redes de telecomunicaciones sin permiso del propietario o administrador autorizado.

Este acceso puede realizarse de forma física o remota y normalmente tiene la finalidad de obtener beneficios personales, económicos o estratégicos. Los delincuentes informáticos pueden aprovechar errores humanos, fallas de software o debilidades de seguridad para ingresar a los sistemas.

Existen diferentes modalidades de acceso no autorizado:

- Robo o descubrimiento de contraseñas.
- Ataques mediante virus y malware.
- Ingeniería social y engaños digitales.
- Espionaje informático.
- Manipulación de redes inalámbricas.
- Interceptación de comunicaciones.
- Uso indebido de privilegios internos.

Uno de los métodos más utilizados es la ingeniería social, donde el atacante engaña a empleados o usuarios para obtener información confidencial. Esto demuestra que la seguridad no depende únicamente de programas tecnológicos, sino también del comportamiento humano.

Los accesos no autorizados generan consecuencias graves:

- Pérdida de datos importantes.
- Daños económicos.
- Interrupción de operaciones.
- Pérdida de productividad.
- Daño a la reputación empresarial.
- Demandas o problemas legales.
- Desconfianza de clientes.

En empresas de telecomunicaciones y redes, un ataque puede afectar servicios de internet, telefonía, almacenamiento de datos y monitoreo empresarial, perjudicando a cientos de usuarios.

Tipos de Personas que Realizan Accesos No Autorizados

Existen diversos perfiles relacionados con accesos ilegales:

Hackers maliciosos: buscan vulnerar sistemas para obtener beneficios o causar daños.

Crackers: rompen medidas de seguridad y alteran programas o sistemas.

Espías informáticos: buscan obtener información confidencial.

Empleados internos: algunas intrusiones provienen de personas con acceso autorizado que utilizan sus privilegios de manera indebida.

Grupos delictivos organizados: realizan ataques dirigidos contra empresas para extorsionar o vender información.

El conocimiento de estos perfiles permite a HollyGather desarrollar mejores estrategias de prevención.

Registro para la Empresa

El registro empresarial constituye un mecanismo administrativo y tecnológico que permite mantener control y organización sobre los recursos digitales.

HollyGather utiliza registros para proteger información y controlar el uso adecuado de sus sistemas.

El registro incluye:

- Identificación completa de empleados.
- Asignación de credenciales.
- Registro de horarios.
- Control de permisos.
- Historial de movimientos.
- Inventario de equipos.
- Control de conexiones externas.

Estos registros funcionan como evidencia administrativa y técnica, permitiendo rastrear incidentes de seguridad.

Un sistema sin registros adecuados dificulta la investigación de incidentes y aumenta la vulnerabilidad empresarial.

Importancia del Registro Empresarial

El registro empresarial no solo tiene una función de control, sino también preventiva.

Sus beneficios son:

- Mayor seguridad.

- Organización administrativa.
- Protección patrimonial.
- Supervisión de actividades.
- Detección de anomalías.
- Cumplimiento legal.

Gracias a estos mecanismos, HollyGather puede garantizar transparencia y protección en los servicios que ofrece.

Registro para el Usuario

El registro del usuario es una herramienta esencial de autenticación y responsabilidad.

Cada usuario posee una identidad digital que permite controlar su acceso y acciones.

Las políticas de HollyGather consideran:

- Usuarios únicos.
- Contraseñas complejas.
- Renovación periódica.
- Autenticación multifactor.
- Recuperación segura.
- Restricciones de acceso.

La finalidad es garantizar que cada persona responda por sus actividades dentro del sistema.

Responsabilidad del Usuario

Los usuarios también tienen obligaciones de seguridad:

- No compartir contraseñas.
- Cerrar sesiones.
- Reportar anomalías.
- Respetar políticas internas.
- Proteger información confidencial.

La seguridad informática es una responsabilidad compartida entre empresa y usuario.

Medidas para Evitar la Entrada a los Equipos de Cómputo

La prevención de accesos ilegales requiere medidas tecnológicas, administrativas y humanas.

Entre las medidas aplicadas por HollyGather destacan:

Antivirus y antimalware: identifican amenazas y bloquean software dañino.

Firewall: filtra conexiones sospechosas.

Actualización constante: corrige vulnerabilidades.

Contraseñas seguras: reducen riesgos de robo de acceso.

Autenticación en dos factores: agrega protección adicional.

Control físico: restringe áreas sensibles.

Cifrado: protege información almacenada y transmitida.

Monitoreo continuo: permite detectar incidentes rápidamente.

Capacitación constante: educa al personal.

Copias de seguridad: facilitan recuperación de información.

Estas medidas forman una estrategia integral de ciberseguridad.

Consecuencias del Acceso No Autorizado

Cuando ocurre un acceso ilegal, las consecuencias pueden ser severas:

- Robo financiero.
- Filtración de información.
- Paralización de servicios.
- Costos de recuperación.
- Pérdida de clientes.
- Afectaciones legales.

Algunas empresas incluso enfrentan cierre temporal de operaciones.

Artículo 367 al 370 del Código Penal Federal

El artículo 367 establece el delito de robo y protege el patrimonio de personas y organizaciones.

En el ámbito tecnológico puede relacionarse con robo de computadoras, servidores, memorias y dispositivos digitales.

Para HollyGather, este artículo justifica controles estrictos sobre los equipos.

Artículo 368 del Código Penal Federal

El artículo 368 contempla conductas equiparadas al robo.

Esto incluye aprovechamiento ilegal de recursos y medios de transmisión.

En telecomunicaciones puede relacionarse con conexiones clandestinas o uso no autorizado de infraestructura.

Artículo 369 del Código Penal Federal

El artículo 369 establece que el delito se consuma al tener posesión del objeto.

En seguridad informática, la obtención ilegal de datos o archivos puede representar daño aun cuando la información sea recuperada.

Artículo 370 del Código Penal Federal

Este artículo define sanciones según el valor del daño.

Las multas y penas aumentan dependiendo de la gravedad y del perjuicio ocasionado.

Esto resalta la importancia económica y legal de proteger equipos e información.

Aplicación en la Empresa HollyGather

HollyGather aplica estos principios mediante políticas de seguridad física y digital.

Entre sus estrategias destacan:

- Monitoreo de redes.
- Auditorías.
- Respaldo de información.
- Control de acceso.
- Protección de servidores.
- Mantenimiento preventivo.
- Protocolos de emergencia.

La empresa también realiza revisiones periódicas para evaluar vulnerabilidades y actualizar sus sistemas de protección.

Esto permite brindar confianza y seguridad a las empresas distribuidoras con las que

trabaja.

Relación del Tema con la Empresa y la Carrera

El acceso no autorizado se relaciona directamente con HollyGather porque la empresa desarrolla actividades vinculadas con instalación y mantenimiento de redes y telecomunicaciones.

También se relaciona con la carrera porque el profesional necesita comprender amenazas, implementar soluciones y actuar con ética y responsabilidad.

El estudio de este tema fortalece conocimientos técnicos y legales, permitiendo diseñar sistemas más seguros y eficientes para las empresas actuales.

Federal relativo al robo de equipo

Nuestra empresa escogio este tema porque representa una base legal fundamental para proteger los equipos tecnológicos dentro de cualquier organización en México. El robo de equipos de cómputo y comunicaciones es uno de los riesgos más frecuentes y costosos, ya que no solo implica la pérdida física de dispositivos, sino también la exposición indebida de toda la información sensible que contienen. Conocer el marco normativo federal aplicable permite comprender claramente las consecuencias legales de estos actos, así como contar con las herramientas necesarias para prevenirlos, denunciarlos y actuar con seguridad. Además, está directamente ligado a mi formación, ya que une el ámbito técnico con la normativa vigente, algo esencial para cualquier profesional dedicado a las redes y la seguridad informática.

A nivel federal en México, este tipo de conductas se encuentran reguladas dentro del Código Penal Federal y demás ordenamientos complementarios, donde se tipifica como delito el apoderamiento ilegítimo de equipos tecnológicos, sistemas, redes o cualquier dispositivo destinado al procesamiento, almacenamiento o transmisión de datos. También se vincula estrechamente con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, ya que el robo de estos equipos casi siempre trae consigo el riesgo de filtrar o usar indebidamente la información confidencial de clientes o usuarios. La legislación define con claridad las sanciones correspondientes, que van desde multas importantes hasta penas de prisión, aumentando su gravedad cuando afectan a instituciones públicas, empresas o cuando se utilizan estos bienes para cometer otros ilícitos como fraude o espionaje. Asimismo, establece la obligación de las organizaciones de implementar medidas de seguridad adecuadas para evitar estos sucesos, quedando sujetas a responsabilidad si no actúan con la diligencia requerida por la ley.

En nuestra empresa lo aplicariamos con las siguientes medidas de seguridad:

- Pondriamos políticas de contraseñas complejas, con requisitos de longitud y cambio periódico. También usariamos el uso de autenticación de dos factores para acceder a sistemas, redes y cuentas corporativas.

- Elaborariamos un reglamento que establezca las normas de uso, traslado y cuidado de los equipos informáticos, así como las sanciones por mal uso, pérdida o robo por negligencia.

- Realizariamos cursos periódicos para enseñar a los empleados cómo cuidar los equipos, cómo reportar situaciones sospechosas y cuáles son sus responsabilidades en materia de seguridad.

- Definiriamos quién es el encargado de cada equipo, cada empleado será responsable del dispositivo que le sea asignado, y deberá firmar un acuse de recibo al recibirlo.

Con todo lo anterior de este tema para la empresa, ajustarse a este marco normativo significa operar con total respaldo legal, evitando multas de gran monto y daños reputacionales muy difíciles de reparar. Y para mi carrera, este tema me sirve para aprender sobre las consecuencias que puede pasar si alguien se roba un equipo de computo en el laboratorio.

Equipo de cómputo en la infraestructura de redes

Elegí este tema porque el equipo de cómputo es el corazón de cualquier sistema de información y la herramienta básica con la que trabajamos todos los días. En el mundo del soporte y la instalación de redes, las computadoras no son solo pantallas para navegar; son los nodos de control, los servidores que procesan los datos y las terminales de trabajo donde se opera todo. Para mí, como estudiante de informática, entender a fondo el hardware, saber qué componentes elegir y cómo optimizar los equipos es fundamental. Si no conocemos las capacidades y limitantes del equipo físico, es imposible diseñar una red que funcione rápido, aguante la carga de trabajo y no dé problemas a cada rato.

Cuando hablamos de equipo de cómputo en un entorno profesional y de redes, no nos referimos únicamente a la computadora de escritorio común. El concepto abarca toda una variedad de hardware especializado que cumple funciones específicas dentro de una arquitectura conectada. Para entenderlo de manera clara, los componentes y equipos clave se dividen en tres áreas grandes:

- Servidores y estaciones de trabajo de alto rendimiento: Son computadoras diseñadas para aguantar jornadas de trabajo pesadas de 24/7. Cuentan con procesadores multinúcleo potentes, gran cantidad de memoria RAM con soporte de corrección de errores y almacenamiento en arreglos discos rápidos para administrar bases de datos, sistemas de inventarios y servicios de red sin detenerse.

- Componentes de hardware esenciales: La elección de elementos como las tarjetas de interfaz de red (NIC), el tipo de almacenamiento (unidades de estado sólido NVMe para velocidad crítica) y una buena ventilación definen si una máquina va a responder rápido o si se va a convertir en un cuello de botella que alente todo el tráfico de la empresa.

• Ciclo de mantenimiento y actualización: Las computadoras sufren desgaste físico por acumulación de polvo o fallas de pasta térmica, y obsolescencia lógica debido a las actualizaciones de software. Un buen plan de hardware requiere calendarizar limpiezas internas, monitorear la salud de los componentes y planear renovaciones de equipo antes de que ocurra una falla catastrófica.

Llevar el control del equipo de cómputo en un proyecto del tamaño de Soriana requiere un orden absoluto, ya que un solo equipo que falle puede detener las cajas de cobro o el sistema de inventarios de una tienda entera. En mi empresa aplicaríamos el tema mediante tres acciones prácticas:

• Homologación y selección de hardware adecuado: Nos aseguraríamos de que los equipos de cómputo usados para el monitoreo de red y los servidores locales en las sucursales tengan las características técnicas exactas para soportar el flujo de datos. No podemos usar equipos caseros; meteríamos hardware de grado empresarial con tarjetas de red dedicadas de alta velocidad.

• Mantenimiento preventivo estricto a las terminales: Diseñaríamos un calendario de mantenimiento físico y lógico para las computadoras de las tiendas conectadas a nuestra red. Mantener los equipos limpios, con buen flujo de aire y libres de software basura asegura que las tarjetas de red funcionen al cien y que no haya caídas de enlace por culpa de una máquina trabada.

• Configuración de respaldos y redundancia: En los servidores de red que instalemos para Soriana, configuraríamos sistemas de almacenamiento espejo (RAID) y fuentes de poder redundantes en el equipo de cómputo. Si un disco duro o una pieza llega a fallar físicamente, el equipo debe seguir operando con la otra parte sin que se pierda la conexión de la tienda ni se detengan las ventas.

La relación aquí es total y directa. Mi carrera en Informática me da la base teórica para

entender la arquitectura de las computadoras, saber cómo interactúa el sistema operativo con los componentes físicos y cómo diagnosticar fallas de hardware. Por otro lado, mi empresa de Redes es el negocio que usa ese conocimiento para armar e interconectar estos equipos de cómputo en el mundo real, haciendo que se comuniquen de manera eficiente en empresas grandes como Soriana. Y el tema del equipo de cómputo es el punto de unión: es el objeto físico sobre el cual aplicamos la informática y la materia prima que mi empresa necesita configurar para que la red de internet tenga sentido.

5- Para cerrar, creo que darle la importancia que merece al equipo de cómputo es una parte clave de la ética profesional. Como informáticos, no se vale recomendar equipo barato o de mala calidad solo por salir del paso, sabiendo que a la larga le va a dar problemas al cliente. Cuando manejas la infraestructura de una empresa como Soriana, ofrecer un diagnóstico honesto sobre qué computadoras se necesitan y mantener el hardware en un estado óptimo es sinónimo de calidad. Al final del día, cuidar el equipo de cómputo es cuidar la estabilidad del negocio, los empleos de la gente que lo usa y la seguridad de la información que viaja por nuestras redes.

Telecomunicaciones

Como dueño de Hollygather, empresa dedicada al diseño, operación y administración de redes de conexión para la transmisión y distribución de información, contenido y servicios digitales hacia grandes cadenas comerciales como Soriana, reconozco que las telecomunicaciones son el pilar fundamental de toda mi operación. Este área no solo define la forma en que conecto sistemas y traslado datos, sino que determina la calidad, seguridad y alcance del servicio que ofrezco. En este reporte presento el análisis de los principios esenciales de las telecomunicaciones, explicando por qué los elegí, su significado, cómo los aplico día a día en mi empresa y la relación directa que tienen con mi negocio y mi desarrollo profesional.

Elegí los principios de las telecomunicaciones porque son la base técnica y funcional sobre la cual existe Hollygather. Mi modelo de negocio consiste precisamente en ofrecer infraestructura y servicios de conexión para que empresas como Soriana reciban y gestionen información de manera continua, rápida y segura. Sin el conocimiento y aplicación correcta de estos principios, no podría garantizar que los datos, materiales o contenidos que distribuimos lleguen correctamente a cada sucursal o sistema del cliente.

Lo seleccioné por razones estratégicas y operativas clave para mí como empresario.

Es la esencia de mi servicio. Mi empresa no vende productos físicos, vende conectividad y transmisión. Todo lo que prometo a Soriana depende directamente de cómo aplique las reglas y fundamentos de las telecomunicaciones.

Seguridad y continuidad. Al trabajar con una empresa del tamaño de Soriana, cualquier fallo en la red genera pérdidas económicas, retrasos y pérdida de confianza.

Ventaja competitiva. Al aplicar estos principios correctamente, puedo ofrecer mayor

velocidad, cobertura, seguridad y soporte especializado.

Cumplimiento normativo y técnico. Me permite operar dentro del marco legal y técnico adecuado.

Las telecomunicaciones se definen como la transmisión de información entre dos o más puntos mediante medios físicos o digitales.

Principio de transmisión y medio: se requiere un emisor, receptor, mensaje y canal.

Principio de señal y codificación: la información se convierte en señales comprensibles para los sistemas.

Principio de ancho de banda: determina la cantidad de datos transmitidos.

Principio de enrutamiento: los datos buscan la mejor ruta dentro de la red.

Principio de seguridad: protege la información contra accesos no autorizados.

Principio de interconexión: permite que diferentes sistemas trabajen juntos.

Diseño redes según la necesidad del cliente.

Uso protocolos y estándares abiertos.

Gestiono rutas para evitar fallas.

Implemento seguridad con cifrado.

Monitoreo constantemente el sistema.

Capacito a mi equipo técnico.

Hollygather depende completamente de estos principios.

Me permiten tomar decisiones inteligentes y comunicarme con expertos.

Desarrollo una visión estratégica para el crecimiento.

Los principios de telecomunicaciones son el corazón de Hollygather y la base de mi desarrollo profesional.

Garantía de los bienes informáticos

En el presente reporte abordaremos la importancia, normativa y aplicación de las garantías para los bienes informáticos dentro de una organización, así como las responsabilidades que implica su adquisición, uso, cuidado y resguardo, vinculándolo con el marco legal y las buenas prácticas en la gestión de tecnologías de la información El tema de garantía de bienes informáticos se enmarca dentro de la regulación de la gestión de tecnologías de la información, y se relaciona con normativas como la Ley Federal de Protección al Consumidor, la Ley Federal de Derechos de Autor, códigos civiles y normativas internas empresariales.

Estas reglas definen los derechos y obligaciones entre proveedores, usuarios y la organización respecto a la calidad, funcionamiento, reparación y sustitución de equipos de cómputo, telecomunicaciones, software y servicios asociados. También se vincula con políticas de asignación, seguridad física y mantenimiento, elementos clave para proteger la inversión y asegurar la continuidad de las operaciones. Para nuestra empresa hollygather, dedicada a redes informáticas, soporte y soluciones tecnológicas, las garantías de bienes informáticos son fundamentales.

Al adquirir, usar o proveer equipos, licencias y servicios, debemos conocer qué cubre cada garantía, por cuánto tiempo y qué responsabilidades tenemos ante fallos o daños. Esto nos permite: reducir riesgos económicos, responder con rapidez ante problemas técnicos, cumplir con compromisos con nuestros clientes y proteger los activos que utilizamos para brindar nuestros servicios.

Entender este tema nos ayuda a actuar con seguridad, cumplir la ley y ofrecer confianza a quienes trabajan con nosotros. Comprender estas normas y políticas nos permite evitar conflictos, gestionar mejor los recursos y garantizar que todo bien

informático cumpla con su función durante su vida útil. La garantía de bienes informáticos es el compromiso legal o contractual por el cual el fabricante, proveedor o vendedor responde ante la organización o usuario por defectos de fabricación, fallos en el funcionamiento, vicios ocultos o incumplimiento de especificaciones técnicas de los equipos, programas o servicios adquirí

- Alcance: Define qué cubre la garantía (reparación, sustitución, devolución o ajustes), qué queda excluido (daños por mal uso, accidentes, modificaciones no autorizadas, condiciones inadecuadas de operación) y el tiempo de vigencia. Carmona Martínez María Fernanda

- Marco legal: Según la Ley Federal de Protección al Consumidor, los bienes nuevos deben contar con garantía mínima, y los contratos deben establecer condiciones claras. Para software, se aplican también reglas sobre licencias y derechos de uso.

- Políticas internas: En la organización, se definen reglas sobre cómo se asignan los bienes, quién es responsable de su cuidado, cómo se reportan fallos y cómo se tramitan las garantías ante proveedores.

También se vincula con la seguridad física: controles de acceso, condiciones de temperatura, humedad, energía y limpieza, ya que si el equipo se daña por no respetar estas normas, la garantía puede perderse. - Mantenimiento: El mantenimiento preventivo y correctivo forma parte de conservar la validez de la garantía, ya que muchas veces es requisito para que esta siga vigente. La garantía protege tanto la inversión económica como la operación diaria, asegurando que los equipos y sistemas funcionen como se espera. En el entorno tecnológico, la garantía aplica a todo tipo de bienes: computadoras, servidores, equipos de red, teléfonos, licencias de software, sistemas de almacenamiento, etc. En hollygather , esto se traduce en: - Verificar condiciones de garantía antes de comprar o contratar. - Llevar registros de fechas,

términos y contactos de proveedores. - Capacitar al personal sobre el uso correcto para no invalidar la garantía. - Cumplir con requisitos de instalación, energía, refrigeración y seguridad física. - Tramitar reparaciones o cambios de forma ágil para no detener los servicios. Esto demuestra que la gestión tecnológica no solo es técnica, sino también administrativa y legal, ya que se trata de proteger activos y derechos. Justificación del tema Elegimos este tema porque la garantía es un mecanismo esencial de protección para cualquier organización que usa tecnología. Conocer sus reglas nos permite exigir calidad, resolver problemas sin costos extra y definir responsabilidades claras entre la empresa, los usuarios y los proveedores. Sin esta información, corremos el riesgo de perder inversiones, sufrir interrupciones en el servicio o enfrentar problemas legales. Además, está directamente relacionado con la asignación, cuidado y seguridad de los bienes informáticos, temas centrales en nuestra actividad. Carmona Martínez María Fernanda En los servicios que ofrecemos, aplicar y respetar las garantías nos ayuda a ser más confiables, reducir riesgos y mantener nuestros sistemas y los de nuestros clientes en óptimas condiciones. Relación con la empresa y la formación académica La relación es muy directa: - Se vincula con adquisición y contratación: saber negociar y revisar términos de garantía al comprar o contratar servicios informáticos. - Se conecta con asignación y control: definir quién usa cada equipo, cómo se cuida y quién responde por él. - Se relaciona con seguridad física: condiciones de acceso, energía, temperatura, humedad y prevención de riesgos, ya que estas condiciones son requisito para mantener la garantía. - Se une con mantenimiento: acciones para conservar el equipo y hacer válida la garantía. Desde el punto de vista académico, este tema forma parte de materias como gestión de tecnologías, normatividad informática, administración de activos, seguridad informática y ética profesional. Esto demuestra que trabajar con tecnologías requiere no solo conocimientos técnicos, sino también dominio de las reglas administrativas, legales y operativas para proteger los bienes y derechos de la organización.

Sistema de cableado estructurado

Es la infraestructura de cables conectados, q el dispositivo integra los servicios de voz, datos y videos de algún edificio q mantiene una conexión a diferentes dispositivos incluyendo:

Cámaras, computadoras interruptoras de seguridad al igual q las conexiones de todos los aparatos necesarios en una empresa.

El sistema de cableado estructurado es aquella q se necesita muy bien estructurar ya que se ocupa mucho para la estructura de los cables de las conexiones de cada puerto de las computadoras o alguna red de conexión flexible a las circunstancias de la empresa un ejemplo es de q en nuestra empresa se dará una implementación de Reuters y swithes etc..

La implementación conexión de cables estructurados lo implementaríamos de una manera en la que la empresa funcione un ejemplo seria las conexiones de las redes LAN, alguna computadora o servicio, también al igual q las conexión de cámaras.

Pues tendría mayormente mucha relación en las dos ya q en la empresa estructuraríamos bien los cables para q tengamos dificultades en la supervisión de las conexiones y mediante la carrera pues se llevaría mucho acabo a q es lo mismo q la empresa nomas q con la diferencia q la aprenderíamos la función de cada uno y sus puertos q conlleva.

Manejo de Equipos de Comunicación

El manejo de equipos de comunicación es una actividad fundamental dentro de cualquier empresa que dependa de la tecnología y del intercambio constante de información. Consiste en la instalación, administración, supervisión, configuración y mantenimiento de dispositivos que permiten la transmisión de datos entre diferentes equipos y usuarios. Gracias a estos sistemas, las organizaciones pueden desarrollar sus operaciones de manera eficiente, mantener conectadas sus áreas de trabajo y asegurar la comunicación digital.

En la actualidad, los equipos de comunicación son indispensables porque prácticamente todas las actividades empresariales requieren acceso a internet, redes internas y sistemas digitales. Desde el envío de correos electrónicos hasta el almacenamiento de archivos y la comunicación entre departamentos, todo depende del correcto funcionamiento de la infraestructura tecnológica.

Las empresas modernas necesitan redes estables y seguras para operar correctamente. Cuando existe una falla en los equipos de comunicación, se pueden presentar problemas como pérdida de información, interrupción de servicios, disminución de productividad y retrasos en procesos administrativos y comerciales.

Tipos de Equipos de Comunicación

Los equipos de comunicación forman parte de la infraestructura tecnológica y cada uno tiene funciones específicas.

Routers

Los routers son dispositivos encargados de dirigir el tráfico de datos entre redes diferentes. Su principal función es determinar la mejor ruta para enviar información hacia internet o hacia otra red. Estos equipos permiten que múltiples dispositivos

compartan una misma conexión y mantienen organizada la comunicación digital.

En Hollygather, los routers son esenciales porque permiten administrar el flujo de datos y garantizar conexiones estables para los clientes.

Switches

Los switches conectan dispositivos dentro de una red local. A diferencia de otros equipos, envían la información directamente al dispositivo que la necesita, mejorando la velocidad y eficiencia de la comunicación.

Los switches son utilizados para conectar computadoras, impresoras, servidores y otros equipos dentro de oficinas o empresas, facilitando el intercambio de recursos y archivos.

Módems

Los módems permiten la comunicación con el proveedor de internet mediante la conversión de señales digitales y analógicas. Sin este dispositivo no sería posible acceder a servicios en línea ni mantener comunicación externa.

La calidad del módem influye directamente en la velocidad y estabilidad de internet, por lo que su mantenimiento y actualización son importantes.

Puntos de Acceso Inalámbricos

Estos dispositivos proporcionan conexión Wi-Fi y permiten que celulares, tabletas y laptops accedan a la red sin utilizar cables.

El uso de puntos de acceso facilita la movilidad dentro de la empresa y mejora la flexibilidad laboral, aunque también requiere medidas adicionales de seguridad para evitar accesos indebidos.

Servidores

Los servidores almacenan y administran datos, programas y recursos compartidos. Son considerados el centro de operaciones digitales porque permiten guardar información importante y controlar servicios internos.

Un servidor puede contener bases de datos, archivos de empleados, sistemas administrativos y plataformas de trabajo.

Cableado Estructurado

El cableado estructurado es parte importante del sistema de comunicación. Se trata del conjunto de cables y conexiones físicas que permiten la transmisión estable de datos.

Una mala instalación del cableado puede generar pérdida de señal, lentitud o fallas constantes en la red.

Importancia del Manejo Adecuado

El manejo adecuado de equipos de comunicación es importante porque asegura el funcionamiento continuo de la empresa. Cuando los equipos son administrados correctamente, se reducen fallas y se optimizan recursos tecnológicos.

Entre sus beneficios se encuentran:

- Mayor velocidad de comunicación.
- Menor riesgo de fallas técnicas.
- Protección de la información empresarial.
- Mejor coordinación entre departamentos.
- Incremento en la productividad.
- Reducción de costos por reparaciones.

La falta de control sobre estos equipos puede ocasionar problemas graves como pérdida de información, caídas del sistema y afectaciones económicas.

Instalación y Configuración

La instalación correcta es el primer paso para garantizar un funcionamiento eficiente. Este proceso incluye la ubicación adecuada de dispositivos, conexión del cableado, asignación de direcciones de red y configuración de parámetros de seguridad.

La configuración implica personalizar los equipos de acuerdo con las necesidades empresariales. Esto puede incluir control de usuarios, administración del ancho de banda y restricciones de acceso.

Una mala configuración puede dejar vulnerabilidades que faciliten ataques o interrupciones.

Mantenimiento Preventivo y Correctivo

El mantenimiento preventivo busca evitar fallas antes de que aparezcan. Incluye limpieza de equipos, monitoreo de temperatura, revisión del cableado y actualización de programas.

El mantenimiento correctivo se realiza cuando el problema ya existe y requiere reparación inmediata.

Ambos tipos de mantenimiento son necesarios para prolongar la vida útil de los equipos y garantizar continuidad operativa.

Seguridad en los Equipos de Comunicación

La seguridad informática es uno de los aspectos más importantes.

Las empresas enfrentan amenazas como:

- Virus informáticos.
- Malware.
- Robo de información.
- Ataques cibernéticos.
- Accesos no autorizados.
- Espionaje digital.

Para prevenir estos riesgos se aplican medidas como:

- Contraseñas robustas.
- Firewalls.
- Antivirus.
- Actualizaciones permanentes.
- Copias de seguridad.
- Monitoreo constante de red.

Estas medidas ayudan a proteger datos y mantener la estabilidad de los servicios.

Fallas Comunes en Equipos de Comunicación

Los equipos pueden presentar problemas debido al desgaste o mala administración.

Entre las fallas más frecuentes se encuentran:

- Sobrecalentamiento.
- Daño físico en cables.
- Configuración incorrecta.

- Saturación de red.
- Fallas eléctricas.
- Obsolescencia tecnológica.

Detectar estas fallas oportunamente evita pérdidas económicas y retrasos.

Aplicación en Hollygather

En Hollygather, el manejo de equipos de comunicación es parte fundamental del servicio que ofrece la empresa. Las actividades incluyen instalación de redes, configuración de routers y switches, mantenimiento de infraestructura tecnológica y supervisión permanente del funcionamiento.

La empresa también implementa sistemas de seguridad y monitoreo para garantizar conectividad estable y proteger la información de los clientes.

Gracias a estas acciones, Hollygather puede ofrecer soluciones tecnológicas confiables y adaptadas a las necesidades de distintas organizaciones.

Relación del Tema con la Empresa y la Carrera

El manejo de equipos de comunicación está directamente relacionado con Hollygather porque representa el núcleo de sus operaciones tecnológicas. Sin estos sistemas sería imposible diseñar redes o brindar servicios especializados.

También guarda relación con la carrera de informática y redes porque desarrolla habilidades de instalación, configuración, mantenimiento y protección de infraestructura tecnológica.

Estos conocimientos preparan al estudiante para enfrentar retos reales en empresas y

fortalecer su desempeño profesional dentro del sector tecnológico.

Políticas y Normas para el Uso de Redes LAN y Manejo de Equipos de Comunicación en la Empresa Hollygather

Políticas para el Manejo de Equipos de Comunicación y Uso de Redes LAN

1. Uso exclusivo para actividades de Hollygather

Los equipos de comunicación y la red LAN deberán utilizarse únicamente para actividades laborales y operativas de la empresa.

2. Acceso autorizado a la red

Solo el personal autorizado podrá utilizar routers, switches, servidores y demás equipos conectados a la red LAN.

3. Mantenimiento preventivo obligatorio

Todos los equipos de comunicación deberán recibir mantenimiento preventivo periódico para evitar fallas y garantizar estabilidad.

4. Protección de información transmitida

La información que circule por la red LAN deberá mantenerse protegida mediante medidas de seguridad y control de acceso.

5. Actualización constante de equipos

Los dispositivos de comunicación deberán mantenerse actualizados con software y firmware vigentes.

6. Supervisión y monitoreo de la red

Hollygather realizará monitoreo continuo del tráfico de red para detectar fallas o actividades sospechosas.

7. Control de dispositivos conectados

Ningún equipo externo podrá conectarse a la red LAN sin autorización previa del área responsable.

8. Respaldo de configuraciones y datos

Se deberán realizar copias de seguridad de configuraciones y archivos importantes para evitar pérdidas de información.

9. Responsabilidad compartida del cuidado del equipo

Todo empleado deberá proteger y utilizar correctamente los equipos asignados.

10. Aplicación de medidas de seguridad informática

La empresa implementará firewalls, antivirus y protocolos de seguridad para proteger la infraestructura tecnológica.

Normas para el Uso de Redes LAN y Equipos de Comunicación

1. No compartir usuarios ni contraseñas

Las credenciales de acceso a la red y a los equipos son personales e intransferibles.

2. No modificar configuraciones sin autorización

Los usuarios no podrán cambiar parámetros de routers, switches o servidores sin permiso del área técnica.

3. No desconectar cableado o dispositivos

Se prohíbe retirar o alterar conexiones físicas de la red LAN sin supervisión autorizada.

4. Mantener equipos encendidos solo cuando sea necesario

Los equipos deberán apagarse correctamente cuando no estén en uso para prolongar su vida útil.

5. No instalar software no autorizado

Queda prohibida la instalación de programas que puedan afectar la red o los equipos.

6. Reportar fallas inmediatamente

Cualquier anomalía en routers, switches, Wi-Fi o red LAN deberá reportarse al área correspondiente.

7. Evitar el acceso a páginas inseguras

No se permitirá ingresar a sitios que representen amenazas para la seguridad de la red.

8. Mantener antivirus y sistemas actualizados

Todo equipo conectado deberá contar con protección activa y actualizaciones recientes.

9. Respetar la privacidad y seguridad de la información

No se deberá acceder o manipular información sin autorización.

10. Seguir protocolos de seguridad y mantenimiento

Todos los usuarios deberán cumplir los procedimientos establecidos por Hollygather para el manejo adecuado de equipos de comunicación.

Estas políticas y normas permiten que Hollygather mantenga una red LAN segura y funcional, garantizando el correcto manejo de los equipos de comunicación, reduciendo

riesgos tecnológicos y fortaleciendo la continuidad de las operaciones empresariales.

Uso de servicio ininterrumpido de corriente

Nosotros elegimos este tema ya que todos los equipos: routers, switches, servidores, sistemas de respaldo y centros de datos dependen totalmente de un suministro eléctrico estable y seguro. El servicio interrumpido de corriente representa una situación que, si no se maneja ni se utiliza conforme a la ley, puede generar fallas graves, daños costosos en la infraestructura tecnológica

El Servicio Ininterrumpido de Corriente (UPS o SAI) es un dispositivo eléctrico que cuenta con baterías recargables internas, diseñado para suministrar energía de forma inmediata cuando se produce un corte en el suministro eléctrico comercial, así como para regular el voltaje y eliminar interferencias o ruidos en la red eléctrica.

Se divide principalmente en dos funciones clave:

- Estabilización: Protege contra subidas o caídas de voltaje, que son muy comunes y dañinas para tarjetas madre, fuentes de poder y discos duros. Actúa como un filtro para que la energía que reciben los equipos sea siempre limpia y segura.

- Autonomía: Al faltar la luz, sus baterías entran en acción automáticamente, brindando energía por un tiempo limitado (desde unos minutos hasta varias horas, según su capacidad). Esto evita que los equipos se apaguen de golpe, permitiendo que los programas finalicen procesos, se guarden archivos abiertos y se realice un apagado ordenado del sistema.

Nuestra empresa aplicaria las siguientes medidas:

- Se instalará un UPS de capacidad media o alta, que cubra todo el rack de servidores, almacenamiento y comunicaciones, asegurando que si ocurre algo

tener un respaldo

- Se respetarán las normas de instalación, usando los cables adecuados y evitando sobrecargar los enchufes.
- cada 6 meses verificar el estado de las baterías, limpieza de ventilación y pruebas de descarga, ya que las baterías tienen vida útil y deben cambiarse antes de que dejen de funcionar.
- - Capacitaremos al personal para que sepan qué hacer cuando se active el UPS (trabajar con calma, guardar archivos y esperar aviso) y qué cosas NO deben conectar a estos dispositivos.

Nuestra empresa también hizo un listado de 10 políticas y 10 normas para el uso de redes LAN

1. Política de acceso: Solo el personal autorizado por la dirección de la empresa podrá acceder a la red LAN, y se asignarán permisos según el cargo y las funciones de cada trabajador.

2. Política de seguridad: La red se protegerá con medidas de seguridad (contraseñas, cortafuegos, antivirus) para evitar accesos no autorizados, virus o ataques informáticos.

3. Política de uso exclusivo: La red se utilizará únicamente para actividades relacionadas con las tareas y objetivos de la empresa; no se permiten usos personales que no estén relacionados con el trabajo.

4. Política de mantenimiento: Se realizarán revisiones, actualizaciones y reparaciones periódicas de la red por parte del departamento de informática o personal capacitado, para garantizar su buen funcionamiento.

5. Política de protección de datos: Toda la información que se transmita o almacene en la red será confidencial, y se respetarán las normativas de protección de datos vigentes.

6. Política de gestión de recursos: El ancho de banda y los recursos de la red se administrarán de forma equitativa, priorizando las actividades que son fundamentales para el funcionamiento de la empresa.

7. Política de conexión de dispositivos: Solo se podrán conectar a la red los dispositivos autorizados por la empresa; no se permite conectar equipos externos sin la aprobación correspondiente.

8. Política de actualizaciones: El software y los sistemas de la red se mantendrán actualizados con las últimas versiones y parches de seguridad, para evitar fallos o vulnerabilidades.

9. Política de reporte de fallos: Cualquier problema, fallo o anomalía en la red debe ser reportado inmediatamente al área de informática para su solución oportuna.

10. Política de formación: Se capacitará al personal en el uso correcto de la red, así como en las buenas prácticas de seguridad y uso responsable de los recursos.

1. Usar contraseñas seguras: Cada usuario debe crear contraseñas complejas (con letras, números y símbolos) y cambiarlas periódicamente; no se deben compartir con otras personas.

2. No modificar configuraciones: Está prohibido cambiar ajustes de la red, direcciones IP, parámetros de seguridad o configuraciones de equipos sin autorización.

3. No descargar contenido no autorizado: No se podrán descargar archivos, programas o contenido de sitios web que no estén relacionados con el trabajo, ni materiales que sean ilegales o dañinos.

4. Respetar el ancho de banda: Se debe hacer un uso moderado de recursos que consuman mucha velocidad (como descargas masivas o transmisiones en línea) para no afectar el trabajo de otros compañeros.

5. No introducir dispositivos ajenos: No se conectarán discos duros, memorias USB o equipos externos que no hayan sido revisados y autorizados por el departamento de informática.

6. Cuidar los equipos de red: Se debe mantener en buen estado los cables, routers, switches y otros dispositivos de red; no se manipularán ni moverán sin necesidad.

7. No enviar información confidencial por canales inseguros: Los datos sensibles se transmitirán a través de vías seguras, evitando correos electrónicos o servicios que no garanticen la privacidad.

8. Reportar actividades sospechosas: Si se detecta un acceso extraño, un error en el sistema o una actividad que parezca irregular, se debe notificar de inmediato al área de tecnología.

9. Apagar equipos correctamente: Al finalizar la jornada, se apagarán los dispositivos conectados a la red de forma adecuada, siguiendo los procedimientos establecidos.

10. Cumplir con las normativas: Todos los usuarios deben respetar estas normas y las leyes vigentes sobre uso de tecnologías y protección de la información.

Para finalizar este tema tiene relación con mi empresa y mi carrera ya que en ambos usamos equipos de computos y esto me permite saber que cosas puedo andar conectando y cuales no

Uso de servicio ininterrumpido de corriente

Nosotros elegimos este tema ya que todos los equipos: routers, switches, servidores, sistemas de respaldo y centros de datos dependen totalmente de un suministro eléctrico estable y seguro. El servicio interrumpido de corriente representa una situación que, si no se maneja ni se utiliza conforme a la ley, puede generar fallas graves, daños costosos en la infraestructura tecnológica

El Servicio Ininterrumpido de Corriente (UPS o SAI) es un dispositivo eléctrico que cuenta con baterías recargables internas, diseñado para suministrar energía de forma inmediata cuando se produce un corte en el suministro eléctrico comercial, así como para regular el voltaje y eliminar interferencias o ruidos en la red eléctrica.

Se divide principalmente en dos funciones clave:

- Estabilización: Protege contra subidas o caídas de voltaje, que son muy comunes y dañinas para tarjetas madre, fuentes de poder y discos duros. Actúa como un filtro para que la energía que reciben los equipos sea siempre limpia y segura.

- Autonomía: Al faltar la luz, sus baterías entran en acción automáticamente, brindando energía por un tiempo limitado (desde unos minutos hasta varias horas, según su capacidad). Esto evita que los equipos se apaguen de golpe, permitiendo que los programas finalicen procesos, se guarden archivos abiertos y se realice un apagado ordenado del sistema.

Nuestra empresa aplicaria las siguientes medidas:

- Se instalará un UPS de capacidad media o alta, que cubra todo el rack de servidores, almacenamiento y comunicaciones, asegurando que si ocurre algo

tener un respaldo

- Se respetarán las normas de instalación, usando los cables adecuados y evitando sobrecargar los enchufes.
- cada 6 meses verificar el estado de las baterías, limpieza de ventilación y pruebas de descarga, ya que las baterías tienen vida útil y deben cambiarse antes de que dejen de funcionar.
- - Capacitaremos al personal para que sepan qué hacer cuando se active el UPS (trabajar con calma, guardar archivos y esperar aviso) y qué cosas NO deben conectar a estos dispositivos.

Nuestra empresa también hizo un listado de 10 políticas y 10 normas para el uso de redes LAN

1. Política de acceso: Solo el personal autorizado por la dirección de la empresa podrá acceder a la red LAN, y se asignarán permisos según el cargo y las funciones de cada trabajador.

2. Política de seguridad: La red se protegerá con medidas de seguridad (contraseñas, cortafuegos, antivirus) para evitar accesos no autorizados, virus o ataques informáticos.

3. Política de uso exclusivo: La red se utilizará únicamente para actividades relacionadas con las tareas y objetivos de la empresa; no se permiten usos personales que no estén relacionados con el trabajo.

4. Política de mantenimiento: Se realizarán revisiones, actualizaciones y reparaciones periódicas de la red por parte del departamento de informática o personal capacitado, para garantizar su buen funcionamiento.

5. Política de protección de datos: Toda la información que se transmita o almacene en la red será confidencial, y se respetarán las normativas de protección de datos vigentes.

6. Política de gestión de recursos: El ancho de banda y los recursos de la red se administrarán de forma equitativa, priorizando las actividades que son fundamentales para el funcionamiento de la empresa.

7. Política de conexión de dispositivos: Solo se podrán conectar a la red los dispositivos autorizados por la empresa; no se permite conectar equipos externos sin la aprobación correspondiente.

8. Política de actualizaciones: El software y los sistemas de la red se mantendrán actualizados con las últimas versiones y parches de seguridad, para evitar fallos o vulnerabilidades.

9. Política de reporte de fallos: Cualquier problema, fallo o anomalía en la red debe ser reportado inmediatamente al área de informática para su solución oportuna.

10. Política de formación: Se capacitará al personal en el uso correcto de la red, así como en las buenas prácticas de seguridad y uso responsable de los recursos.

1. Usar contraseñas seguras: Cada usuario debe crear contraseñas complejas (con letras, números y símbolos) y cambiarlas periódicamente; no se deben compartir con otras personas.

2. No modificar configuraciones: Está prohibido cambiar ajustes de la red, direcciones IP, parámetros de seguridad o configuraciones de equipos sin autorización.

3. No descargar contenido no autorizado: No se podrán descargar archivos, programas o contenido de sitios web que no estén relacionados con el trabajo, ni materiales que sean ilegales o dañinos.

4. Respetar el ancho de banda: Se debe hacer un uso moderado de recursos que consuman mucha velocidad (como descargas masivas o transmisiones en línea) para no afectar el trabajo de otros compañeros.

5. No introducir dispositivos ajenos: No se conectarán discos duros, memorias USB o equipos externos que no hayan sido revisados y autorizados por el departamento de informática.

6. Cuidar los equipos de red: Se debe mantener en buen estado los cables, routers, switches y otros dispositivos de red; no se manipularán ni moverán sin necesidad.

7. No enviar información confidencial por canales inseguros: Los datos sensibles se transmitirán a través de vías seguras, evitando correos electrónicos o servicios que no garanticen la privacidad.

8. Reportar actividades sospechosas: Si se detecta un acceso extraño, un error en el sistema o una actividad que parezca irregular, se debe notificar de inmediato al área de tecnología.

9. Apagar equipos correctamente: Al finalizar la jornada, se apagarán los dispositivos conectados a la red de forma adecuada, siguiendo los procedimientos establecidos.

10. Cumplir con las normativas: Todos los usuarios deben respetar estas normas y las leyes vigentes sobre uso de tecnologías y protección de la información.

Para finalizar este tema tiene relación con mi empresa y mi carrera ya que en ambos usamos equipos de computos y esto me permite saber que cosas puedo andar conectando y cuales no

Uso de servicio ininterrumpido de corriente

Nosotros elegimos este tema ya que todos los equipos: routers, switches, servidores, sistemas de respaldo y centros de datos dependen totalmente de un suministro eléctrico estable y seguro. El servicio interrumpido de corriente representa una situación que, si no se maneja ni se utiliza conforme a la ley, puede generar fallas graves, daños costosos en la infraestructura tecnológica

El Servicio Ininterrumpido de Corriente (UPS o SAI) es un dispositivo eléctrico que cuenta con baterías recargables internas, diseñado para suministrar energía de forma inmediata cuando se produce un corte en el suministro eléctrico comercial, así como para regular el voltaje y eliminar interferencias o ruidos en la red eléctrica.

Se divide principalmente en dos funciones clave:

- Estabilización: Protege contra subidas o caídas de voltaje, que son muy comunes y dañinas para tarjetas madre, fuentes de poder y discos duros. Actúa como un filtro para que la energía que reciben los equipos sea siempre limpia y segura.

- Autonomía: Al faltar la luz, sus baterías entran en acción automáticamente, brindando energía por un tiempo limitado (desde unos minutos hasta varias horas, según su capacidad). Esto evita que los equipos se apaguen de golpe, permitiendo que los programas finalicen procesos, se guarden archivos abiertos y se realice un apagado ordenado del sistema.

Nuestra empresa aplicaria las siguientes medidas:

- Se instalará un UPS de capacidad media o alta, que cubra todo el rack de servidores, almacenamiento y comunicaciones, asegurando que si ocurre algo tener un respaldo

- Se respetarán las normas de instalación, usando los cables adecuados y evitando sobrecargar los enchufes.
- cada 6 meses verificar el estado de las baterías, limpieza de ventilación y pruebas de descarga, ya que las baterías tienen vida útil y deben cambiarse antes de que dejen de funcionar.
- - Capacitaremos al personal para que sepan qué hacer cuando se active el UPS (trabajar con calma, guardar archivos y esperar aviso) y qué cosas NO deben conectar a estos dispositivos.

Nuestra empresa también hizo un listado de 10 políticas y 10 normas para el uso de redes LAN

1. Política de acceso: Solo el personal autorizado por la dirección de la empresa podrá acceder a la red LAN, y se asignarán permisos según el cargo y las funciones de cada trabajador.

2. Política de seguridad: La red se protegerá con medidas de seguridad (contraseñas, cortafuegos, antivirus) para evitar accesos no autorizados, virus o ataques informáticos.

3. Política de uso exclusivo: La red se utilizará únicamente para actividades relacionadas con las tareas y objetivos de la empresa; no se permiten usos personales que no estén relacionados con el trabajo.

4. Política de mantenimiento: Se realizarán revisiones, actualizaciones y reparaciones periódicas de la red por parte del departamento de informática o personal capacitado, para garantizar su buen funcionamiento.

5. Política de protección de datos: Toda la información que se transmita o almacene en la red será confidencial, y se respetarán las normativas de protección de datos

vigentes.

6. Política de gestión de recursos: El ancho de banda y los recursos de la red se administrarán de forma equitativa, priorizando las actividades que son fundamentales para el funcionamiento de la empresa.

7. Política de conexión de dispositivos: Solo se podrán conectar a la red los dispositivos autorizados por la empresa; no se permite conectar equipos externos sin la aprobación correspondiente.

8. Política de actualizaciones: El software y los sistemas de la red se mantendrán actualizados con las últimas versiones y parches de seguridad, para evitar fallos o vulnerabilidades.

9. Política de reporte de fallos: Cualquier problema, fallo o anomalía en la red debe ser reportado inmediatamente al área de informática para su solución oportuna.

10. Política de formación: Se capacitará al personal en el uso correcto de la red, así como en las buenas prácticas de seguridad y uso responsable de los recursos.

1. Usar contraseñas seguras: Cada usuario debe crear contraseñas complejas (con letras, números y símbolos) y cambiarlas periódicamente; no se deben compartir con otras personas.

2. No modificar configuraciones: Está prohibido cambiar ajustes de la red, direcciones IP, parámetros de seguridad o configuraciones de equipos sin autorización.

3. No descargar contenido no autorizado: No se podrán descargar archivos, programas o contenido de sitios web que no estén relacionados con el trabajo, ni

materiales que sean ilegales o dañinos.

4. Respetar el ancho de banda: Se debe hacer un uso moderado de recursos que consuman mucha velocidad (como descargas masivas o transmisiones en línea) para no afectar el trabajo de otros compañeros.

5. No introducir dispositivos ajenos: No se conectarán discos duros, memorias USB o equipos externos que no hayan sido revisados y autorizados por el departamento de informática.

6. Cuidar los equipos de red: Se debe mantener en buen estado los cables, routers, switches y otros dispositivos de red; no se manipularán ni moverán sin necesidad.

7. No enviar información confidencial por canales inseguros: Los datos sensibles se transmitirán a través de vías seguras, evitando correos electrónicos o servicios que no garanticen la privacidad.

8. Reportar actividades sospechosas: Si se detecta un acceso extraño, un error en el sistema o una actividad que parezca irregular, se debe notificar de inmediato al área de tecnología.

9. Apagar equipos correctamente: Al finalizar la jornada, se apagarán los dispositivos conectados a la red de forma adecuada, siguiendo los procedimientos establecidos.

10. Cumplir con las normativas: Todos los usuarios deben respetar estas normas y las leyes vigentes sobre uso de tecnologías y protección de la información.

Para finalizar este tema tiene relación con mi empresa y mi carrera ya que en ambos usamos equipos de computos y esto me permite saber que cosas puedo andar conectando y cuales no

ADQUISICIÓN DE PROGRAMAS DE CÓMPUTO

Elegí este tema porque la adquisición de software es el punto de partida legal y operativo para cualquier proyecto tecnológico serio. Muchas veces la gente piensa que dar soporte o instalar redes se limita a tirar cable, conectar switches y configurar routers, pero la realidad es que el software de gestión, los sistemas operativos de red y los esquemas de licenciamiento son los que controlan toda esa infraestructura. Para mí, como estudiante de informática, dominar los procesos de compra y selección de software corporativo es fundamental. Si compramos las licencias equivocadas, podemos hacer que la empresa gaste de más, que sufra problemas de compatibilidad o que termine metida en un problema legal gordo.

La adquisición de programas de cómputo en el ámbito corporativo va mucho más allá de simplemente descargar una aplicación y usarla. Involucra un análisis detallado de costos, necesidades del negocio, tipos de licencias y el soporte que ofrece el proveedor. Los puntos clave que debemos entender sobre este proceso son los siguientes:

- Modelos de licenciamiento corporativo: Hoy en día las empresas ya casi no compran software de forma perpetua. Todo se maneja a través de esquemas SaaS (Software como Servicio) con suscripciones mensuales o anuales, licenciamiento por volumen para empresas con muchas sucursales, o licencias por número de núcleos y usuarios concurrentes. Elegir el modelo adecuado cambia por completo el presupuesto técnico.

- Cumplimiento legal y auditorías (Compliance): Adquirir software original implica firmar contratos de uso (EULA) que determinan exactamente en qué máquinas y entornos se puede ejecutar el programa. Las grandes corporaciones están expuestas a auditorías periódicas; si se detecta que hay más instalaciones activas que licencias pagadas, las multas pueden detener la operación por completo.

- Criterios de evaluación técnica: Antes de adquirir cualquier software para una infraestructura de red, se debe evaluar la escalabilidad, la compatibilidad con el

hardware existente, la frecuencia de parches de seguridad que lanza el fabricante y que cuente con un acuerdo de nivel de servicio (SLA) que garantice soporte técnico inmediato ante fallas críticas.

Para una empresa del tamaño de Soriana, con cientos de tiendas y un flujo de información masivo, la adquisición de programas no puede tomarse a la ligera. En mi empresa aplicaríamos este tema con tres estrategias operativas muy claras:

- Gestión centralizada de licencias de red: Al comprar el software de monitoreo de tráfico, los sistemas operativos de servidores y los firewalls perimetrales para Soriana, negociaríamos contratos corporativos por volumen. Esto nos permite tener un control centralizado desde un panel general para activar, renovar o dar de baja las licencias de cada sucursal de manera automática y ordenada.

- Validación estricta antes de la compra (Fase de Pruebas): Antes de adquirir de manera definitiva cualquier software para la red de Soriana, haríamos pruebas piloto en laboratorios cerrados. Necesitamos asegurarnos de que el nuevo programa no interfiera con los sistemas internos de cobro, inventarios o bases de datos que la tienda ya usa, evitando pérdidas de dinero por incompatibilidad.

- Implementación de software de seguridad homologado: Aseguraríamos la adquisición legítima de software especializado en ciberseguridad para los endpoints y servidores locales de las sucursales. Al comprar soluciones originales directamente con los distribuidores autorizados, garantizamos que la red de Soriana tenga acceso a actualizaciones de firmas de virus en tiempo real para proteger las transacciones bancarias.

La conexión aquí es perfecta y cierra el ciclo profesional de nuestro trabajo. Mi carrera en Informática me da el criterio técnico para analizar las especificaciones del software, entender la diferencia entre arquitecturas de sistemas y saber qué licencias son

compatibles. Mi empresa de Redes aprovecha este conocimiento informático para seleccionar y gestionar de forma inteligente los programas con los que operará la conectividad de clientes grandes como Soriana. Y el tema de la adquisición de programas es el puente regulador: es la vía legal y estratégica mediante la cual mi empresa obtiene las herramientas de software necesarias para aplicar lo que aprendí en la carrera de forma segura, eficiente y sin riesgos legales.

Como conclusión, considero que la adquisición correcta y honesta de programas es un pilar fundamental de la ética profesional en tecnología. Como informáticos, tenemos la responsabilidad de guiar al cliente para que adquiera herramientas legítimas y transparentes, rechazando cualquier solución dudosa o pirata que abarate costos a corto plazo pero destruya la seguridad del negocio después. Cuando trabajas con la red de una cadena masiva como Soriana, la legalidad del software que adquieres define el nivel de profesionalismo de tu empresa. Hacer los procesos bien desde la compra es la única forma de garantizar un entorno estable, proteger la información de millones de clientes y construir un nombre respetable en el mercado de soporte técnico.

Licenciamiento de Software

Como dueño de Hollygather, empresa dedicada al diseño, operación y administración de redes de conexión para distribuir información, contenido y soluciones digitales a empresas como Soriana, entiendo que el software es el motor que hace funcionar toda nuestra infraestructura y los servicios que entregamos. El licenciamiento de software es el marco legal y técnico que regula el uso, distribución y manejo de estas herramientas digitales, y es indispensable para operar con seguridad, legalidad y responsabilidad. En este reporte explico por qué elegí este tema, su contenido detallado, cómo lo aplico en cada proceso de mi empresa y la relación directa que tiene con mi negocio y mi desarrollo profesional.

Elegí el tema del licenciamiento de software porque es un pilar esencial para la operación y sostenibilidad de Hollygather. Mi negocio consiste en conectar sistemas y llevar soluciones digitales a clientes como Soriana, y todo lo que hacemos depende de programas, plataformas y aplicaciones que están protegidos por derechos de autor y normativas de uso.

Lo seleccioné por razones clave para mi empresa y mi forma de trabajar Seguridad jurídica total. Al ser proveedor de una empresa grande y regulada como Soriana, cualquier uso indebido o sin licencia de software nos expone a ambos a sanciones graves, multas, demandas o suspensiones de servicio. Elegir este tema me permite garantizar que todo lo que instalamos, operamos o distribuimos está autorizado legalmente, evitando cualquier riesgo legal para mí y para mis clientes.

Calidad y funcionamiento garantizado. El software que cuenta con licenciamiento oficial recibe actualizaciones, soporte técnico, parches de seguridad y mejoras constantes. Esto es vital para mí, porque necesito que mis redes funcionen sin fallos, que la información se transmita de forma segura y que los servicios que doy a Soriana sean

estables y confiables. Usar software sin licencia es correr el riesgo de tener errores, virus o falta de funcionamiento en cualquier momento.

Confianza y reputación empresarial. Para ser un socio estratégico de empresas como Soriana, debo demostrar que opero bajo normas éticas y legales estrictas. El manejo correcto de licencias demuestra profesionalismo, orden y compromiso, características que hacen que mis clientes confíen en mí y prefieran mis servicios por encima de la competencia.

Cumplimiento normativo. En México y a nivel internacional, existen leyes estrictas que protegen los programas informáticos. Conocer y aplicar las reglas de licenciamiento es la única forma de operar dentro del marco legal, evitar problemas con autoridades y mantener la validez de mi modelo de negocio.

En resumen, lo elegí porque es la única manera de asegurar que Hollygather funcione legalmente, con calidad y con la confianza que mis clientes requieren.

El licenciamiento de software es el contrato o autorización legal mediante el cual el creador o titular de los derechos de un programa informático le da permiso a una persona o empresa para usarlo, bajo condiciones específicas, claras y limitadas. No significa comprar el programa, sino comprar el derecho a usarlo respetando las reglas que establece su fabricante.

Concepto y naturaleza. El software es una obra protegida por la Ley Federal del Derecho de Autor y tratados internacionales. La licencia especifica qué se puede y qué no se puede hacer con él, incluyendo duración, número de usuarios, equipos y uso permitido.

Tipos de licencias. Existen licencias perpetuas, por suscripción, por usuario, por equipo, por volumen y de distribución. Cada una tiene diferentes condiciones y costos.

Derechos y obligaciones. El fabricante otorga derechos como instalación, soporte y actualizaciones. El usuario debe respetar límites de uso, evitar copias ilegales y no modificar ni distribuir sin autorización.

Ámbito de distribución. Para empresas como la mía, es fundamental contar con licencias que permitan la redistribución cuando el software forma parte del servicio entregado al cliente.

Consecuencias del incumplimiento. El uso ilegal puede generar multas, sanciones, pérdida del servicio y riesgos técnicos como virus o fallos.

Inventario y control total: Mantengo un registro detallado de todo el software.

Selección y contratación adecuada: Elijo licencias acorde a las necesidades empresariales.

Cumplimiento con Soriana: Incluyo información de licencias en contratos y garantizo legalidad.

Seguridad y actualizaciones: Mantengo sistemas actualizados.

Capacitación: Mi equipo conoce las reglas y políticas internas.

Gestión ante auditorías: Tengo documentación organizada.

Relación con mi empresa: El licenciamiento garantiza operación legal, calidad del servicio y confianza del cliente.

Relación con mi carrera: Me permite tomar decisiones estratégicas, generar confianza y tener una visión integral del negocio.

El licenciamiento de software es esencial para unir la legalidad con la calidad técnica. Es la base para el éxito de Hollygather y mi crecimiento profesional.

INSTALACIÓN Y/O ACTUALIZACIÓN DE PROGRAMAS DE

CÓMPUTO

Este tema se refiere al conjunto de procedimientos, pasos y normas necesarios para incorporar nuevos programas de cómputo en los equipos informáticos, así como para modificar o reemplazar las versiones que ya están instaladas por otras más recientes o mejoradas. La instalación implica preparar el equipo, verificar requisitos, ejecutar el proceso de carga del programa, configurarlo según el uso que se le dará y comprobar que funcione correctamente. Por su parte, la actualización consiste en incorporar mejoras, correcciones de errores, cambios en las funciones o parches de seguridad que el desarrollador del software lanza después de su salida al mercado, lo que puede incluir cambios pequeños o renovaciones completas del programa. También abarca aspectos como la verificación de licencias, la compatibilidad con otros sistemas, el respaldo de información antes de iniciar cualquier cambio y la validación del funcionamiento posterior.

Significa que estas acciones son procesos de cambio y mejora continua en la infraestructura tecnológica. Instalar o actualizar no es solo poner un programa en el equipo, sino asegurar que la herramienta sea legal, compatible, segura y útil para la tarea que se va a realizar. Representa la responsabilidad de mantener los recursos informáticos actualizados y funcionales, evitando que la tecnología se vuelva obsoleta o insegura. Además, implica que estas actividades requieren planeación, conocimiento y control, ya que cualquier error puede interrumpir el trabajo diario, exponer la información a amenazas o generar gastos no previstos. En esencia, significa mantener la capacidad operativa de la empresa a través de herramientas que cumplen con los estándares de calidad, seguridad y rendimiento necesarios.

Para aplicar este tema de forma efectiva y ordenada, establecería un procedimiento estructurado que incluya las siguientes acciones:

- Planificación previa: Antes de cualquier instalación o actualización, evaluar qué programas son necesarios, si cumplen con los requisitos técnicos de los equipos, si son compatibles con otros sistemas que ya se usan y si cuentan con las licencias correspondientes para su uso legal. También se define el momento adecuado para realizar el cambio, evitando horarios de alta actividad para no interrumpir las operaciones.
- Resguardo de información: Realizar copias de seguridad de todos los archivos, configuraciones y datos que puedan verse afectados, para recuperarlos en caso de que ocurra algún fallo durante el proceso.
- Ejecución controlada: Realizar la instalación o actualización siguiendo las indicaciones del fabricante, configurando cada programa según las funciones que realizará el usuario y asignando los permisos de acceso correspondientes. En casos de cambios importantes, se puede probar primero en un equipo de prueba para detectar problemas antes de extenderlo a toda la empresa.
- Verificación y validación: Una vez terminado el proceso, comprobar que el programa abre correctamente, realiza sus funciones sin errores y se integra bien con las demás herramientas. Se verifica también que no haya quedado información antigua o archivos innecesarios que ocupen espacio o generen conflictos.
- Gestión de versiones y licencias: Llevar un registro actualizado de qué programas hay instalados, qué versión tienen, cuándo se actualizaron y el estado de sus licencias. Esto ayuda a saber cuándo corresponde renovar o actualizar nuevamente, y evita el uso de programas no autorizados.

La instalación y actualización de programas son procesos esenciales para que el software cumpla su función. Sin una gestión adecuada de estas actividades, las herramientas pierden utilidad, seguridad y rendimiento. Comprender cómo se realizan,

cuáles son sus riesgos y cómo controlarlos permite garantizar que la tecnología sea un apoyo real y no un obstáculo para las actividades diarias.

Mi empresa depende de programas de cómputo para administrar información, realizar operaciones, comunicarse y gestionar recursos. Una correcta instalación asegura que cada área cuente con las herramientas exactas que necesita para trabajar. Las actualizaciones permiten corregir vulnerabilidades que podrían poner en riesgo datos confidenciales, mejorar la velocidad de los procesos y adaptar las herramientas a nuevas necesidades o cambios en las normativas. Además, al controlar estas actividades, se evitan sanciones legales por uso de software sin licencia, se reducen los tiempos muertos por fallos técnicos y se prolonga la vida útil de los equipos, lo que se traduce en ahorros económicos y mayor estabilidad en el funcionamiento general de la organización.

Este tema está directamente vinculado a mi perfil profesional, ya que la capacidad de gestionar la instalación y actualización de programas es una competencia técnica y organizativa muy valorada. Me permite no solo saber realizar estas acciones, sino también planificarlas, controlarlas y optimizarlas, aportando soluciones para mejorar la infraestructura tecnológica. Al dominar este proceso, puedo identificar riesgos, proponer mejoras, asegurar el cumplimiento de normas y contribuir a que la empresa trabaje con herramientas seguras y modernas. Esto fortalece mi capacidad para resolver problemas, me hace un profesional más competente y preparado para asumir responsabilidades en la gestión de recursos informáticos, alineando mi trabajo con los objetivos de eficiencia y seguridad que requiere la organización.

Identificación de la de las políticas y controles aplicables al software y de sistema de una organización

respaldos de información

El respaldo de información, o backup, es el proceso de duplicar y archivar datos con la finalidad de poder recuperarlos en caso de pérdida, daño, robo o eliminación accidental. Es una de las principales medidas de seguridad informática y continuidad operativa dentro de cualquier organización.

Importancia en Hollygather:

Para Hollygather, empresa especializada en redes informáticas y soporte 24/7, la información representa su activo más crítico. Esto incluye configuraciones de equipos, bases de datos de clientes, contratos, bitácoras y documentación técnica. La pérdida de estos datos generaría interrupción de servicios, afectaciones económicas, sanciones legales y daño a la reputación de la empresa.

Política de respaldos en Hollygather: Hollygather implementa la metodología 3-2-1, reconocida internacionalmente como buena práctica en seguridad de la información:

Principio 3-2-1 Aplicación en Hollygather

3 copias de los datos Se conserva el archivo original y dos respaldos adicionales

2 tipos de medios diferentes Almacenamiento en servidor NAS local y en nube privada con cifrado

1 copia externa Respaldo resguardado en un centro de datos externo certificado

Esquema de respaldos:

Respaldo completo: Se ejecuta todos los domingos a las 23:00 horas. Copia la totalidad de la información designada.

Respaldo incremental: Se realiza de lunes a sábado a las 23:00 horas. Únicamente respalda los archivos que fueron creados o modificados durante el día. Respaldo de bases de datos: Los sistemas que contienen información de clientes se respaldan

automáticamente cada 6 horas mediante replicación.

Responsabilidades establecidas:

Departamento de TI de Hollygather: Es responsable de programar, ejecutar y monitorear los respaldos. Debe realizar pruebas de restauración el primer lunes de cada mes para comprobar la integridad de las copias.

Usuarios y colaboradores: Tienen la obligación de guardar toda la información relacionada con su trabajo en las unidades de red asignadas por la empresa, como \ \Servidor_HG\Usuarios. La información almacenada en el Escritorio, carpeta Descargas o disco local C: queda excluida del protocolo de respaldo y su pérdida será responsabilidad del usuario.

Proceso de recuperación de datos:

Si un colaborador requiere restaurar información, deberá solicitarlo al área de Soporte Técnico de Hollygather mediante un ticket, especificando el nombre del archivo, la ubicación original y la fecha aproximada de la última versión. El tiempo estimado de recuperación es de 2 a 4 horas hábiles.

Fundamento legal:

El incumplimiento de estas políticas puede constituir un delito. El artículo 211 Bis del Código Penal Federal sanciona a quien sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática. Asimismo, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares obliga a Hollygather a

implementar medidas de seguridad para evitar la pérdida de datos personales de sus clientes.

La implementación de esta política permite a Hollygather garantizar la disponibilidad, integridad y confidencialidad de la información, reducir riesgos operativos y cumplir con sus compromisos de servicio ante los clientes.

Acceso a Internet

Derechos, usos y marco normativa En el presente documento analizamos el acceso a Internet como un derecho fundamental, su importancia en la vida de las personas, las condiciones que lo regulan, los beneficios que aporta y las responsabilidades que conlleva su uso, así como su aplicación en el ámbito personal, educativo y laboral El acceso a Internet se ha convertido en una herramienta esencial en la actualidad, ya que permite la comunicación, el intercambio de información, el acceso a servicios, la educación y el desarrollo de actividades cotidianas. Este tema se relaciona con normativas nacionales e internacionales que reconocen este derecho, además de reglas técnicas y administrativas que regulan su prestación por parte de proveedores y su uso responsable por parte de los usuarios. También se vincula con la gestión de redes, la seguridad informática y el respeto a los derechos digitales de cada persona. Para María, el acceso a Internet es un recurso fundamental que le facilita múltiples actividades: desde realizar trámites, estudiar, trabajar o mantenerse en contacto con familiares y amigos, hasta acceder a información y servicios que mejoran su calidad de vida. Conocer las condiciones de este acceso, sus derechos como usuaria y las buenas prácticas para su uso, le permite aprovechar al máximo las ventajas de la tecnología, evitar riesgos y actuar de manera responsable en el entorno digital. Entender este tema le ayuda a usar la tecnología de forma segura, eficiente y conforme a las reglas, asegurando que sus actividades en línea sean útiles, legales y protegidas. El acceso a Internet es la posibilidad de conectarse a redes globales de comunicación para intercambiar datos, información y servicios. Se reconoce como un derecho humano en diversos marcos normativos, entre ellos

disposiciones que garantizan el derecho a la información y la libertad de expresión en el entorno digital - Características: Es un medio de conexión que permite acceder a plataformas, contenidos, servicios y comunicaciones en tiempo real, a través de redes de telecomunicaciones y sistemas informáticos. - Marco normativo: Se rige por leyes que regulan la prestación del servicio por parte de empresas proveedoras, las condiciones de contratación, la calidad del servicio, la protección de datos personales y el uso adecuado de la red. También establece Carmona Martínez María Fernanda derechos como la continuidad del servicio, la claridad en los contratos y la protección frente a abusos. - Tipos de uso: Puede ser personal, educativo, laboral o recreativo, y cada uno implica responsabilidades diferentes: al usarla, se debe respetar la ley, la privacidad de otras personas, los derechos de autor y las normas de convivencia digital. - Requisitos: Para acceder, se necesitan equipos de cómputo o dispositivos compatibles, infraestructura de red y un contrato con un proveedor, donde se establecen términos, costos, velocidades y condiciones de uso. El acceso a Internet no es solo una herramienta técnica, sino un derecho que facilita la participación en la sociedad y el desarrollo de actividades en todos los ámbitos. Aplicación en la vida diaria - En la educación: para consultar información, realizar tareas, tomar cursos o acceder a materiales de estudio. - En el trabajo: para realizar actividades laborales, comunicarse con compañeros o clientes, y acceder a herramientas digitales. - En la vida personal: para mantenerse en contacto con seres queridos, realizar trámites administrativos, acceder a servicios de salud, entretenimiento y comercio. Esto demuestra que el acceso a Internet es una herramienta transversal que integra todas las áreas de la vida, y que su uso adecuado requiere tanto conocimientos técnicos como el respeto a las reglas y derechos de los demás. Elegimos este tema porque el acceso a Internet se ha convertido en un elemento indispensable para el desarrollo personal y social. Conocer sus características, derechos y obligaciones permite a las personas

aprovechar sus beneficios, evitar problemas como el uso indebido, los riesgos de seguridad o los abusos en el servicio, y actuar de manera responsable. Además, es un derecho que permite la igualdad de oportunidades, por lo que su comprensión es fundamental para participar plenamente en la sociedad actual. - El conocimiento de las tecnologías de la información y las comunicaciones, y su funcionamiento. - El respeto a los derechos digitales y la normativa que regula el uso de la red. - El desarrollo de habilidades para usar la tecnología de manera segura, eficiente y ética. Carmona Martínez María Fernanda Desde el punto de vista académico, se relaciona con materias como tecnología de la información, ciberseguridad, derecho informático y educación digital. Esto demuestra que el acceso a Internet es mucho más que una conexión técnica: es un derecho que implica conocimientos, responsabilidad y respeto a las reglas que rigen la convivencia en el mundo digital

. Revisión de acceso a internet

revisión de acceso a internet es un proceso de seguridad que verifica q los usuarios,diispositivos aplicación , tengan permisos para q se puedan conectar a una red o servicios de línea . su objetivo de esto es implementar e asegurar la autorización de los recursos de una empresa y poder detectar posibles brechas o algún virus q quisiera acceder a los servicios de seguridad de acceso a internet .

Lo elegí mayormente para q pudiera implementar y optimizar los datos y poder protegerlos , el uso de la infraestructura y también cumplir con algún estándar de seguridad para proteger los recursos necesarios para los datos personales de las personas .

retomando la revisión de acceso a internet en nuestra empresa lo aplicaríamos mayormente en el uso de cada conexión de la red esto conlleva a q la revisión de red lo tendríamos q ir checando para q no tengamos algún fallo con la seguridad de cada servicio de internet , se llevaría acabo con una revisión exhaustiva para mantener un control firme y seguro

mediante la carrera su relación que tiene la revisión de acceso a internet seria checar cada puerto y variedad de los datos como : las ip , los puertos q estén bien conectados y la conectividad de los dispositivos al igual q en la empresa seria lo mismo

Registros de Usuario

Los registros de usuario representan uno de los elementos más importantes dentro de la seguridad informática y la administración de redes empresariales. Consisten en la creación, organización y control de cuentas digitales utilizadas por trabajadores y personas autorizadas para acceder a sistemas, programas, equipos y recursos tecnológicos.

En las empresas modernas, los registros de usuario permiten identificar a cada persona que interactúa con la infraestructura tecnológica. Gracias a este sistema es posible mantener control sobre quién ingresa, qué actividades realiza y qué recursos utiliza dentro de la red empresarial.

En Hollygather, empresa dedicada a redes y conexiones, los registros de usuario forman parte fundamental del control tecnológico porque permiten administrar accesos, proteger información y mantener organizada la operación digital.

Los registros funcionan mediante procesos de autenticación y autorización.

La autenticación consiste en comprobar la identidad del usuario mediante credenciales como nombre de usuario, contraseña, huella digital o códigos de verificación.

La autorización determina qué acciones puede realizar el usuario una vez que ha ingresado al sistema. Esto significa que no todos los usuarios tienen los mismos privilegios o acceso a la información.

Este mecanismo reduce riesgos de seguridad y facilita la administración de los recursos tecnológicos.

Importancia de los Registros de Usuario

El uso de registros de usuario es importante porque ayuda a mantener orden y seguridad dentro de las empresas.

Sin registros adecuados, cualquier persona podría acceder a sistemas, modificar información o utilizar recursos sin control.

Entre las principales funciones e importancia de los registros de usuario se encuentran:

- Identificación individual de usuarios.
- Protección de información confidencial.
- Supervisión de actividades realizadas en la red.
- Control de permisos y privilegios.
- Prevención de accesos no autorizados.
- Organización de recursos tecnológicos.
- Apoyo en auditorías y revisiones de seguridad.

Los registros también permiten conservar evidencia digital de las acciones realizadas por los usuarios. Esto facilita investigaciones internas cuando ocurre pérdida de

información o incidentes de seguridad.

Tipos de Usuarios y Registros

Dentro de las empresas existen diferentes niveles de usuario dependiendo de sus funciones.

Usuario Administrador

Es el responsable del control general del sistema y posee permisos completos.

Entre sus funciones están:

- Configurar servidores y redes.
- Crear y eliminar cuentas.
- Asignar permisos.
- Supervisar actividades.
- Resolver fallas técnicas.

Debido al nivel de acceso que poseen, estas cuentas requieren medidas estrictas de protección.

Usuario Estándar

Tiene acceso limitado únicamente a herramientas necesarias para desarrollar sus funciones.

Estos usuarios pueden trabajar con programas, consultar información y utilizar servicios asignados sin modificar configuraciones críticas.

Usuario Invitado o Temporal

Se utiliza cuando personas externas requieren acceso controlado durante periodos

limitados.

Estos registros reducen riesgos porque restringen privilegios y tiempo de acceso.

Usuarios Remotos

Con el crecimiento del trabajo a distancia, muchas empresas utilizan usuarios remotos que acceden mediante internet y redes privadas.

Este tipo de acceso requiere protocolos adicionales de seguridad.

Proceso de Creación de Registros

La creación de registros debe seguir procedimientos organizados.

Generalmente incluye:

1. Identificación del trabajador.

2. Asignación de usuario.

3. Creación de contraseña inicial.

4. Definición de permisos.

5. Configuración de seguridad.

6. Registro dentro del sistema administrativo.

El proceso debe documentarse para mantener control y evitar duplicidades.

La eliminación o suspensión de cuentas también es importante cuando un trabajador cambia de puesto o deja la empresa.

Seguridad en los Registros de Usuario

La seguridad informática es indispensable porque los registros pueden convertirse en objetivos de ataques digitales.

Entre las amenazas más comunes se encuentran:

Robo de Contraseñas

Ocurre cuando terceros obtienen claves de acceso mediante engaños o programas maliciosos.

Phishing

Consiste en correos o páginas falsas que buscan engañar a los usuarios para obtener credenciales.,

Suplantación de Identidad

Personas no autorizadas utilizan cuentas ajenas para ingresar a sistemas.

Malware y Virus

Programas dañinos pueden robar datos o modificar información.

Ataques de Fuerza Bruta

Se realizan múltiples intentos automáticos para descubrir contraseñas.

Estas amenazas pueden afectar seriamente a la empresa.

Por ello se implementan medidas como:

- Contraseñas robustas.
- Cambios periódicos.
- Antivirus.
- Firewalls.
- Bloqueo automático.
- Monitoreo continuo.

- Cifrado de información.

Administración de Permisos

No todos los empleados necesitan acceso completo.

La administración de permisos permite:

- Limitar información sensible.
- Reducir errores humanos.
- Evitar fugas de datos.
- Mejorar organización.

Existen permisos de lectura, edición, eliminación y administración.

Asignarlos correctamente fortalece la seguridad.

Auditoría y Supervisión

Los registros permiten realizar auditorías.

Una auditoría tecnológica analiza:

- Quién accedió.
- Cuándo accedió.
- Qué modificó.
- Qué recursos utilizó.

Esta supervisión ayuda a detectar anomalías y corregir vulnerabilidades.

Aplicación en Hollygather

Hollygather utiliza registros de usuario para administrar accesos dentro de sus sistemas

y redes.u

Cada trabajador dispone de credenciales individuales para ingresar a plataformas, servidores y herramientas.

La empresa administra permisos dependiendo del área de trabajo.

Los técnicos pueden acceder a configuraciones de red, mientras que otras áreas poseen permisos limitados.

Hollygather también implementa monitoreo de accesos, respaldos y control administrativo para proteger información.

Al brindar servicios de redes y conexiones a otras organizaciones, la empresa puede instalar sistemas de autenticación y administración de usuarios que fortalezcan la seguridad tecnológica.

Esto mejora el control operativo y protege recursos digitales.

Relación del Tema con la Empresa y la Carrera

Los registros de usuario se relacionan directamente con Hollygather porque la empresa depende de sistemas tecnológicos y redes de comunicación.

La administración adecuada de usuarios permite controlar accesos y garantizar protección de información.

Asimismo, este tema se vincula con la carrera de informática y redes porque desarrolla competencias sobre administración de sistemas, seguridad informática y control de infraestructura tecnológica.

El profesional aprende a configurar cuentas, asignar privilegios y supervisar sistemas digitales, habilidades esenciales en el entorno laboral actual.

Políticas para Registros de Usuario en Hollygather

1. Uso obligatorio de cuentas individuales y personales.
2. Contraseñas seguras con actualización periódica.
3. Control y limitación de privilegios de acceso.
4. Suspensión inmediata de cuentas inactivas o no autorizadas.
5. Monitoreo y registro permanente de actividades digitales.

Bitacoras de acceso a los buzones de correo

Elegimos el acceso a los buzones de correo ya que permiten a los usuarios ingresar, consultar, enviar y recibir información a través de las cuentas de correo corporativo, asegurando que solo las personas autorizadas puedan ver o manipular esa información.

Las bitácoras de acceso a los buzones de correo es la herramienta principal de comunicación empresarial, y en él circula información crítica: datos de clientes, contratos, estrategias, facturas y datos confidenciales. Por ello, el acceso debe estar regulado y protegido. Se puede realizar de dos formas principales:

- Acceso local: Desde los equipos de la empresa, mediante programas como Outlook, Thunderbird o clientes de correo instalados en las computadoras.

- Acceso remoto / web: Desde navegadores de internet, dispositivos móviles o equipos externos, lo que brinda movilidad pero aumenta los riesgos de seguridad.

Los riesgos de un acceso mal gestionado incluyen: acceso no autorizado por parte de personas ajenas o empleados sin permiso, robo de información, suplantación de identidad, envío de correos maliciosos, pérdida de mensajes o fugas de datos que pueden dañan la reputación y seguridad de nuestra empresa.

Nosotros para implementar un control seguro y eficiente del acceso a los buzones de

correo, aplicaremos lo siguiente:

- Se creará una cuenta de correo única e intransferible para cada empleado, vinculada a su cargo y área de trabajo.
- Se asignarán permisos diferenciados: un usuario estándar solo accede a su buzón; jefes o directivos pueden tener accesos compartidos o delegados solo si es estrictamente necesario.
- Para accesos desde fuera de la red corporativa o dispositivos personales, se activará la Autenticación de Doble Factor (2FA): además de la contraseña, se requerirá un código temporal enviado al celular o aplicación de seguridad.
- Se bloqueará el acceso desde ubicaciones o países no autorizados, y se restringirá la conexión solo desde dispositivos que cumplan con los requisitos de seguridad de la empresa.

También hicimos un listado de 5 políticas y 5 controles que vamos a implementar en nuestra empresa para el software y el sistema

1. Política de acceso autorizado: Solo podrán acceder al sistema de correo electrónico las personas que cuenten con una cuenta asignada oficialmente por la empresa; queda prohibido compartir cuentas, claves o permitir el ingreso a terceros.

2. Política de contraseñas seguras: Todas las cuentas deben utilizar contraseñas que cumplan con requisitos de complejidad (mayúsculas, minúsculas, números y símbolos), deben cambiarse cada cierto tiempo y nunca deben anotarse en lugares visibles o compartirse.

3. Política de uso exclusivo laboral: El sistema y el software de correo se utilizarán

únicamente para temas relacionados con las actividades, proyectos y objetivos de la empresa; queda prohibido su uso para asuntos personales, envío de contenido ilegal, ofensivo o publicitario no autorizado.

4. Política de seguridad de conexión: El acceso al correo desde redes públicas, dispositivos personales o ubicaciones externas solo se permitirá bajo medidas de seguridad adicionales (como VPN o autenticación doble), y queda prohibido dejar sesiones abiertas o recordar contraseñas en equipos compartidos.

5. Política de custodia y retención: Toda la información enviada o recibida es propiedad de la empresa. Se establecen reglas para guardar, archivar o eliminar correos según normativas legales y de respaldo; no se debe borrar información que sea evidencia de acuerdos o transacciones sin autorización.

1. Control de autenticación de doble factor: Implementado obligatoriamente en el software de correo, requiriendo una segunda prueba de identidad (código SMS, aplicación o llave física) además de la contraseña, para asegurar que quien entra es realmente el usuario autorizado.

2. Control de bloqueo por intentos fallidos: Configurado en el sistema: si se ingresan credenciales incorrectas más de 3 o 5 veces consecutivas, la cuenta se bloquea automáticamente por un tiempo determinado o hasta que la desbloquee el área de TI, evitando ataques de fuerza bruta.

3. Control de registro y auditoría: El sistema guarda un historial detallado de cada acceso: quién ingresó, desde dónde, a qué hora, qué mensajes leyó, envió o borró. Estos registros se revisan periódicamente para detectar comportamientos anómalos.

4. Control de permisos y delegación: Desde la configuración del software, se limita lo

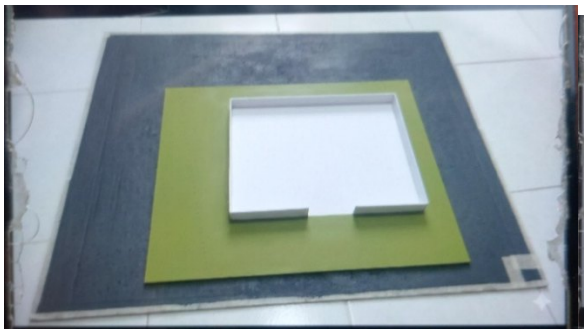
que cada usuario puede hacer: hay controles para impedir el reenvío de correos a cuentas externas, prohibir descargar archivos adjuntos masivos o restringir el acceso a ciertas carpetas compartidas.

5. Control de actualización y mantenimiento: Se programa la actualización automática del software cliente y del servidor de correo con los últimos parches de seguridad, además de análisis continuos de antivirus y antispam integrados al sistema para bloquear accesos o mensajes maliciosos antes de que lleguen al buzón.

Anexo 1 Evidencia de maqueta

Descripción:

La evidencia muestra la representación física y lógica de la infraestructura de red de HollyGather, incluyendo equipos, dispositivos de comunicación y elementos tecnológicos que forman parte de la operación de la empresa.




Objetivo:

Demostrar la correcta integración de los componentes físicos y lógicos de una red, aplicando conocimientos de infraestructura tecnológica y telecomunicaciones.

Evidencia fotográfica

Anexo 2 Conciencia Histórica III

Descripción:

La evidencia incluye gafetes, tarjetas de presentación y materiales promocionales que fortalecen la identidad corporativa de HollyGather.

Objetivo:

Demostrar el uso de recursos visuales e institucionales para proyectar una imagen profesional y consolidar la identidad empresarial.

Gafetes


HOLLYGATHER
Phone Number :
+52 5517918319
Website :
https://hollygather.pagino.mx/
Email Address :
hollygather.pagino.mx
Address :
Vicente Guerrero 2, Ayotla 56560
GUTIERREZ SANCHEZ
GERARDO DAVID
CEO Directo general
HOLLYGATHER
Phone Number :
+52 5517918319
Website :
https://hollygather.pagino.mx/
Email Address :
hollygather.pagino.mx
Address :
Vicente Guerrero 2, Ayotla 56560
MONTIEL CASARROJA
JOSÉ EDUARDO
Ingeniero en redes
HOLLYGATHER
Phone Number :
+52 5517918319
Website :
https://hollygather.pagino.mx/
Email Address :
hollygather.pagino.mx
Address :
Vicente Guerrero 2, Ayotla 56560
CRUZ MERINO
ESMERALDA
Técnico en soportes
HOLLYGATHER
Phone Number :
+52 5517918319
Website :
https://hollygather.pagino.mx/
Email Address :
hollygather.pagino.mx
Address :
Vicente Guerrero 2, Ayotla 56560
CARMONA MARTINEZ
MARIA FERNANDA
Coordinadora general

Tarjetas de presentación

Anexo 3 Formación Socioemocional VI

Descripción:

La evidencia integra redes sociales y material audiovisual utilizado para difundir los servicios y actividades de HollyGather.

Objetivo:

Comprobar la utilización responsable y efectiva de medios digitales para fortalecer la comunicación con los usuarios y la presencia digital de la empresa.

Redes sociales

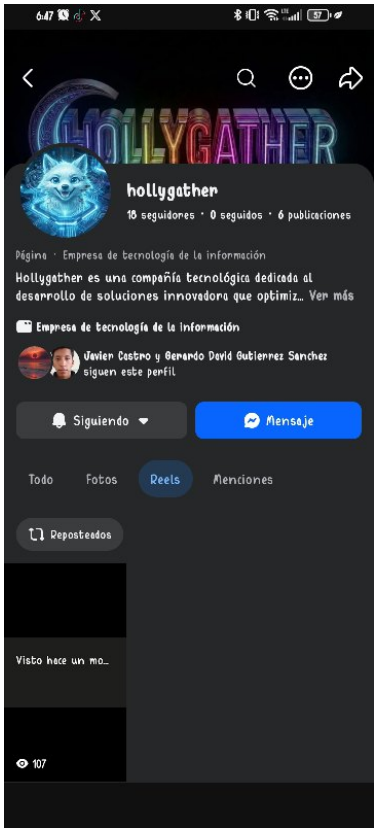

Hollygather
Cuenta de empresa de WhatsApp

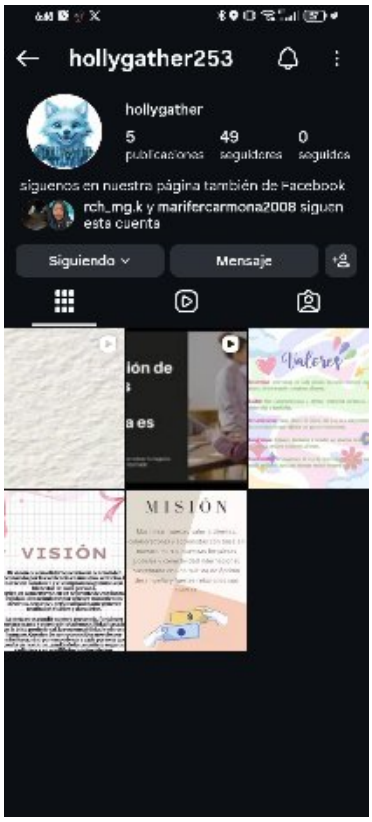

@hollygather.236
Hollygather 236

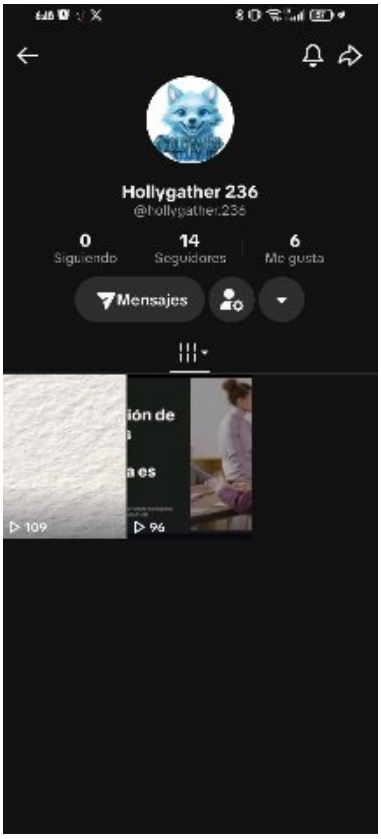

@HOLLYGATHER253


SCAN ME

Publicaciones







Trípticos

¿QUIENES SOMÓS?

Hollygather es una empresa de Redes Telecomunicaciones que se encarga de que tu internet, equipos y comunicación digital funcionen al 100%. Somos los doctores de tu red.

Configuramos firewalls, VPNs y políticas pa' que nadie hackee tu empresa ni se robe datos. Tambien resolvemos cualquier tipo de prolema Virus, robo de información, accesos no autorizados. etc

TELÉFONO
5517918319

CORREO
Hollygather253@gmail.com

SITIO WEB
https://hollygather.pagino.mx/

siganos en nuestras redes sociales

INSTAGRAM
@hollygather253

FACEBOOK
hollygather

TIK TOK
@hollygather236

Conalep 236

602

turno:matutino

P.T.B EN INFORMATICA

¿EN QUÉ TE AYUDA HOLLYGATHER?

"Conectar, proteger y optimizar toda la infraestructura de red de tu empresa, para que tú solo te preocupes por tu negocio."

HERRAMIENTAS PROFESIONALES QUE OCUPAMOS

Seguridad Informática
Cableado Estructurado Certificado
Venta y Configuración de Equipo
Soporte Técnico 24/7

Optimización de la Experiencia del Cliente

1. Reducir el tiempo de respuesta a consultas técnicas a menos de 2 horas para el 90% de nuestros clientes dentro de los próximos 2 meses.

Retención y Enganche del Cliente

2. Incrementar la satisfacción del cliente mediante encuestas post-servicio y planes de mejora continua en nuestra empresa

3. mplementar prácticas de **tecnología sostenible**, como optimización del consumo energético de servidores y equipos de red, locales, fortaleciendo la imagen corporativa y la relación con la sociedad.

SERVICIOS

DIAGNÓSTICO FLUKE GRATIS + REPORTE

INSTALACIÓN WIFI EMPRESARIAL

SOPORTE 24/7 "RED SANA

SEGURIDAD PERIMETRAL CON FORTINET

CCTV INTELIGENTE + CONTROL DE ACCESO

TELEFONÍA IP + CONMUTADOR EN LA NUBE

Anexo 4 Elaboración de páginas web

Descripción:

La evidencia presenta la página web desarrollada para HollyGather, mostrando información institucional, servicios y medios de contacto.

Objetivo:

Demostrar la capacidad de diseñar y desarrollar una plataforma web funcional que fortalezca la presencia digital y facilite la interacción con los clientes.

HollyGather

QR


Diseñamos tecnología que funciona como un sistema.
Hollygather desarrolla soluciones innovadoras orientadas a mejorar la forma en que las empresas interactúan digitalmente y administran sus flujos de información.
Nuestro enfoque está en crear ecosistemas tecnológicos funcionales, conectados y adaptados a cada necesidad — donde cada herramienta, proceso y dato trabajan en conjunto.
INTEGRACIÓN
End-to-end
ENFOQUE
Personalizado
RESULTADO
Operativo

Anexo Temas selectos de matemáticas III

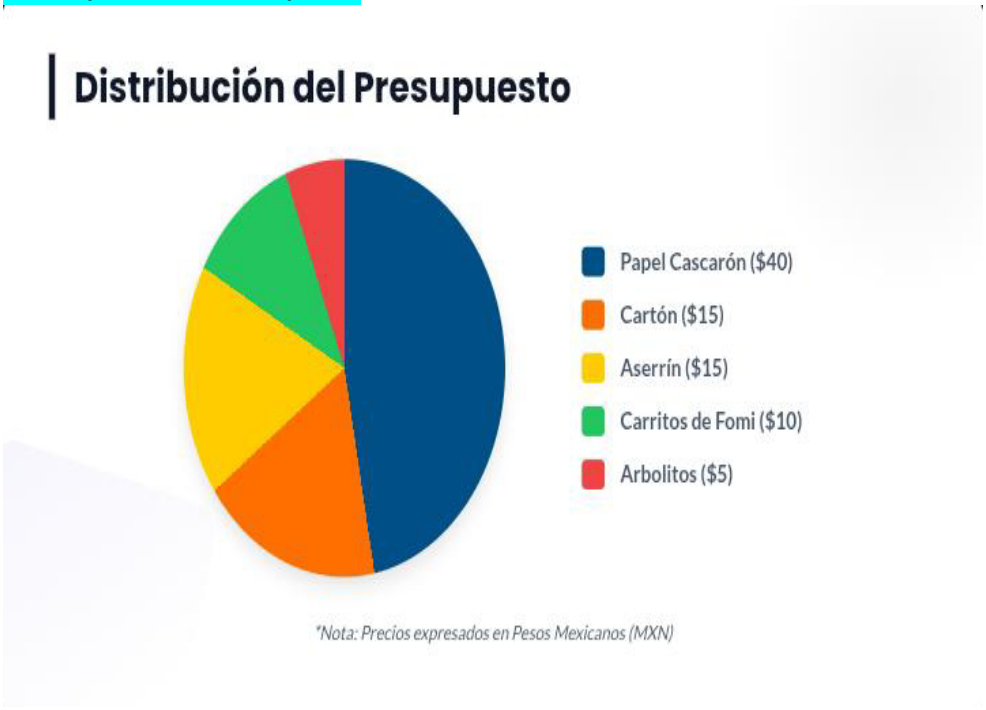
Descripción:

La evidencia presenta el análisis de costos y presupuesto necesarios para la operación de HollyGather, considerando equipos de red, infraestructura tecnológica, materiales, software y recursos requeridos para el funcionamiento de la empresa.

Objetivo:

Demostrar la aplicación de procedimientos matemáticos y financieros para calcular costos, estimar inversiones y analizar la viabilidad económica de HollyGather, permitiendo una adecuada planificación de los recursos necesarios para la prestación de sus servicios de telecomunicaciones y conectividad.

Presupesto de maqueta



Conclusion

La elaboración de HollyGather permitió aplicar de manera práctica los conocimientos adquiridos durante la formación profesional, integrando aspectos técnicos, administrativos y empresariales en una propuesta enfocada en redes y telecomunicaciones.

El desarrollo de la empresa demostró la importancia de la planificación, la seguridad informática, la infraestructura tecnológica y la innovación para ofrecer servicios de calidad.

Asimismo, el proyecto fortaleció habilidades de investigación, análisis, trabajo colaborativo y resolución de problemas, permitiendo comprender el funcionamiento de una organización tecnológica dentro de un entorno real.

HollyGather representa una propuesta empresarial que combina tecnología, conectividad y responsabilidad, contribuyendo al desarrollo digital de usuarios y organizaciones.

Agradecimientos

Gerardo David Gutiérrez Sánchez

Agradezco a mis docentes por compartir sus conocimientos y experiencias, los cuales fueron fundamentales para el desarrollo de este proyecto. También agradezco a mis compañeros de equipo por su colaboración, compromiso y disposición para trabajar en conjunto. De igual manera, reconozco el apoyo de mi familia, que me brindó motivación y respaldo durante este proceso académico. Gracias a todos ellos fue posible fortalecer mis conocimientos y contribuir al desarrollo de HollyGather.

José Eduardo Montiel Casarroja

Agradezco a los profesores que guiaron este proyecto por su dedicación, orientación y apoyo constante durante el desarrollo de las actividades. Asimismo, agradezco a mis compañeros por el trabajo colaborativo y el esfuerzo realizado para alcanzar nuestros objetivos. También expreso mi gratitud a mi familia por impulsarme a seguir adelante y apoyar mi formación profesional. Este proyecto representa el resultado del aprendizaje adquirido gracias a todas las personas que contribuyeron a mi crecimiento académico.

Esmeralda Cruz Merildo

Agradezco profundamente a mis docentes por brindarme las herramientas necesarias para desarrollar este proyecto y fortalecer mis conocimientos en el área tecnológica. También agradezco a mis compañeros de equipo por su cooperación y responsabilidad durante cada etapa del trabajo. De igual forma, agradezco a mi familia por su apoyo incondicional y confianza, factores que me motivan a continuar superándome día con

día.

María Fernanda Carmona Martínez

Agradezco a los docentes por compartir sus conocimientos y fomentar el aprendizaje a través de proyectos que fortalecen nuestras habilidades profesionales. Asimismo, agradezco a mis compañeros por el esfuerzo, la comunicación y el compromiso demostrado durante el desarrollo de HollyGather. También agradezco a mi familia por su apoyo constante y por motivarme a alcanzar mis metas académicas y personales.

Ángel Yael Hernández Gabino

Agradezco a mis profesores por la enseñanza, orientación y acompañamiento brindado durante la realización de este proyecto. Reconozco también el esfuerzo y dedicación de mis compañeros, quienes contribuyeron al cumplimiento de los objetivos planteados. De igual manera, agradezco a mi familia por el respaldo que me ha brindado en mi formación académica y por motivarme a seguir desarrollando mis capacidades profesionales.

Christian Enrique López Rivera

Expreso mi agradecimiento a los docentes que participaron en nuestra formación, ya que sus enseñanzas fueron esenciales para el desarrollo de este proyecto empresarial. Asimismo, agradezco a mis compañeros por el trabajo en equipo, la responsabilidad y la

disposición para colaborar en cada actividad realizada. También agradezco a mi familia por su apoyo y comprensión durante este proceso de aprendizaje y crecimiento personal.

Luis Carlos Lagos Morales

Agradezco a los profesores por compartir sus conocimientos y contribuir a nuestro desarrollo académico mediante actividades que fortalecen nuestras competencias profesionales. También agradezco a mis compañeros por su compromiso, colaboración y apoyo durante la elaboración de este proyecto. Finalmente, agradezco a mi familia por su confianza, motivación y acompañamiento a lo largo de mi formación educativa.

Brandon Zoet Fermín Castañeda

Agradezco a los docentes por su dedicación y por transmitir conocimientos que fueron fundamentales para la realización de este proyecto. Asimismo, agradezco a mis compañeros por su esfuerzo, trabajo colaborativo y disposición para enfrentar los retos presentados durante el desarrollo de HollyGather. De igual forma, agradezco a mi familia por su apoyo constante, el cual ha sido una fuente importante de motivación para continuar alcanzando mis objetivos académicos y profesionales.

Referencias bibiográficas

1. Constitución Política de los Estados Unidos Mexicanos. Cámara de Diputados.

https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

2. Código Penal Federal. Cámara de Diputados.

https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

3. Ley Federal del Derecho de Autor. Cámara de Diputados.

https://www.diputados.gob.mx/LeyesBiblio/pdf/LFDA.pdf

4. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Cámara de Diputados.

https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

5. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

https://home.inai.org.mx

6. Secretaría de Infraestructura, Comunicaciones y Transportes (SICT).

https://www.gob.mx/sct

7. Cisco Networking Academy. Introducción a las Redes.

https://www.netacad.com

8. Cisco Systems. Soluciones de Redes Empresariales.

https://www.cisco.com

9. Tanenbaum, A. S. Redes de Computadoras. Pearson.

https://www.pearson.com

10. Kurose, J. F. y Ross, K. W. Redes de Computadoras: Un Enfoque Descendente. Pearson.

https://www.pearson.com

11. Organización Internacional de Normalización (ISO/IEC 27001).

https://www.iso.org/isoiec-27001-information-security.html

12. Unión Internacional de Telecomunicaciones (UIT).

https://www.itu.int

13. Secretaría de Economía. Propiedad Intelectual y Normatividad Tecnológica.

https://www.gob.mx/se

14. Microsoft Learn. Seguridad Informática y Administración de Redes.

https://learn.microsoft.com

15. Oracle Documentation. Bases de Datos y Seguridad.

https://docs.oracle.com