

Gestión de Proyectos Tecnológicos

Aníbal Mario Mazza Fraquelli

<https://www.linkedin.com/in/fraquelli/>

DIPLOMATURA EN ALTA DIRECCIÓN DE EQUIPOS DE TECNOLOGÍA (ADET)

Índice

- Gestión de Riesgos
 - Gestión
 - Crisis
 - El riesgo operacional
 - La mitigación
 - Risk Frameworks
 - Project Risks en general
- Evaluación y Gestión de proyectos tecnológicos
- Desarrollo de Emprendimientos
 - La carpeta de presentación
- Incubadoras tecnológicas

Gestión de Riesgos

- Componente importante de la operación de toda organización, ya que incluye:
 - detectar,
 - analizar y minimizar cualquier riesgo
 - que pueda impedir el cumplimiento de objetivos
 - o tener repercusiones negativas.
- Técnicas eficaces de gestión de riesgos:
 - manejar las **incertidumbres** y
 - **tomar decisiones informadas** para defender sus intereses.

Gestión de Riesgos

- Ciclo BAU/Crisis/BAU
- La gestión de riesgos es proactiva.
- La gestión de crisis es reactiva a los eventos. (si hay “algo” previsto...) → DR Plan
- Previene las crisis, mientras que las gestiona
- Puede mitigar, lo que interconecta ambas disciplinas



Gestión de Riesgos

- La gestión de riesgos y la gestión de crisis forman un **continuo**.
- La gestión de riesgos ayuda a prevenir catástrofes mediante
 - procesos,
 - protocolos
 - y controles.
- Las organizaciones pueden mitigar las crisis identificando y abordando los riesgos de antemano.
- Puede guiar la respuesta y recuperación ante una crisis. → DRP
- La gestión de riesgos ayuda a las organizaciones a:
 - evaluar la situación,
 - analizar las posibles implicaciones
 - y establecer medidas de respuesta ante crisis.
- Las empresas deben tomar decisiones relacionadas con las crisis, asignar recursos y reducir daños. → el “vamos viendo”...

Gestión de Riesgos

- Un aspecto clave → **elemento tiempo** → **How long?**
- **Gestión de riesgos:**
 - Es un esfuerzo continuo y permanente en situaciones **SIN** crisis.
 - Implica evaluaciones de
 - riesgos regulares,
 - monitoreo y adaptación de las
 - tácticas de respuesta ANTE circunstancias cambiantes. → **Plan actualizado...**
- **Gestión de crisis:**
 - Requiere acción inmediata.
 - Pasos rápidos, coordinación y comunicación para reducir la crisis.
 - La “gente” **adecuada** (no la necesaria y la que tiene que estar...)
 - **Cuando el mar estaba calmo, todos los barcos navegaban con destreza...**

Gestión de Riesgos

- Se enfatiza en la prevención, mitigación y preparación.
- Esto involucra la identificación, análisis y mitigación de riesgos.
- Las estrategias de gestión de riesgos pueden incluir:
 - **Evitar el riesgo:** Eliminar por completo la posibilidad de que ocurra.
 - **Transferir el riesgo:** Transferir la responsabilidad financiera del riesgo a un tercero, como a través de un seguro. → Si es asegurable...
 - **Reducir el riesgo:** Disminuir la probabilidad o el impacto del riesgo.
 - **Aceptar el riesgo:** Tomar una decisión consciente de asumir el riesgo.

Gestión de Riesgos – La crisis

- Se enfatiza en la respuesta, contención y recuperación.
- Esto incluye:
 - Activar planes de respuesta:
 - Poner en marcha protocolos preestablecidos para enfrentar la situación.
 - Establecer canales de comunicación
 - Mantener informados a los grupos de interés de manera clara y oportuna.
 - Trabajar con las partes interesadas:
 - Mantener una comunicación fluida con empleados, clientes, proveedores y otros afectados.
 - Estabilizar y reanudar operaciones:
 - Minimizar las interrupciones y volver a la normalidad lo antes posible.

Gestión de Riesgos



- Cada organización establece sus PROPIOS umbrales

Gestión de Riesgos – Triggers (detonantes)

- Son indicadores de riesgo o señales de alerta
- Son eventos **(reales o potenciales)** o condiciones que sugieren la posibilidad de que un riesgo se materialice.
- Pueden presentarse de diversas formas, dependiendo de la naturaleza del riesgo y la industria. → no es igual aún dentro de la industria
- Pueden ser cuantitativos o cualitativos, internos o externos, e involucrar umbrales o patrones.
 - Un aumento repentino en intentos fallidos de inicio de sesión o en el tráfico de red podría indicar un peligro de ciberseguridad.
 - Las caídas en el precio de las acciones o la volatilidad del mercado pueden desencadenar riesgos de mercado en el sector financiero.
 - El “gerente que se va...” y “se lleva a sus amigos...” → Caso AN
 - “Rumores” de mercado...

Gestión de Riesgos - Estratégicos



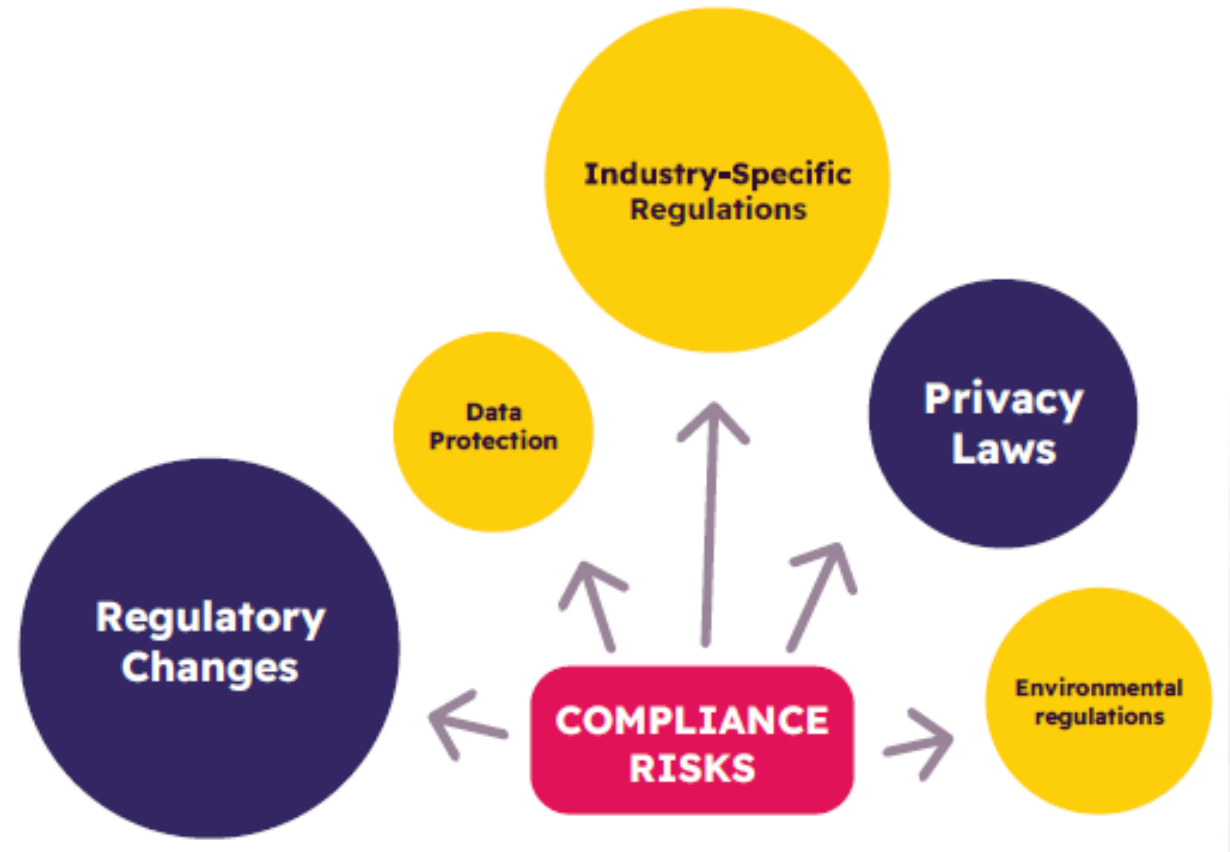
Gestión de Riesgos - Tipos

- Habitualmente se analizan por separado, sin embargo...
 - Se omite la sinergia de riesgos...
 - La “cadena” es tan “fuerte” como el más “débil” de sus eslabones...
 - Cuento chino → se perdió la guerra → el mensaje no llegó → herrero → clavo de mala calidad → herradura del caballo



Gestión de Riesgos - Compliance

- Los riesgos de cumplimiento surgen de la **incapacidad** de una empresa para
 - seguir leyes,
 - regulaciones,
 - estándares
 - o políticas internas.
- Estos peligros pueden costarles
 - dinero,
 - reputación,
 - oportunidades comerciales
 - y generar problemas legales.



Habitualmente, no se presta la DEBIDA atención

Gestión de Riesgos - Regulatorio

- Modificaciones a leyes, regulaciones, políticas o lineamientos que gobiernan industrias y actividades.
- Motivados por actualizaciones legislativas, avances tecnológicos y armonización global.
- Estabilidad “legal” o “para invertir” → Certeza jurídica...
- **Impacto significativo en empresas:**
 - Nuevas obligaciones de cumplimiento, ajustes operativos y cambios en la dinámica del mercado.
- **Gestión Efectiva:**
 - Estar informado a través de monitoreo regulatorio.
 - Realizar evaluaciones de riesgo y desarrollar planes proactivos de cumplimiento.
 - **Aprendizaje y adaptación continuos → planificación estratégica.**
 - Alinear modelos de negocio y estrategias → nuevos requisitos regulatorios.
- **Navegando el Entorno/Contexto:**
 - Monitoreo activo, evaluación y adaptación a cambios regulatorios.
 - Implementar medidas sólidas de cumplimiento.
 - Alinear planes estratégicos con nuevos requisitos regulatorios.
- **Beneficios de la Gestión Efectiva:**
 - Cumplir con las obligaciones legales → Mantener la competitividad en el mercado

Gestión de Riesgos

- **Leyes de Protección de Datos y Privacidad:**

- Restringen la recolección, almacenamiento, procesamiento y transferencia de datos personales por parte de las organizaciones.
- Protegen los datos personales, definen derechos, promueven la transparencia y la rendición de cuentas, y permiten flujos transfronterizos de datos.
- Ley de Habeas Data 25.326 en CAMBIO en Argentina...
 - Historias Clínicas... Mi Argentina... Renaper...

- **Propósitos de las Regulaciones:**

- **Preservar privacidad, confidencialidad, integridad y disponibilidad de los datos.**
- Derechos individuales: acceso, corrección o eliminación de datos y recursos legales por infracciones. → ¿Quién atiende los pedidos de Habeas Data?
- Responsabilidad y transparencia: divulgación de las prácticas de datos.
- Protección de la privacidad en transferencias transfronterizas.

Gestión de Riesgos – Principios Clave

- **Consentimiento informado y expreso para recolección y procesamiento de datos.**
- Limitación de la finalidad: datos adquiridos para propósitos legítimos y no mal uso.
- Minimización de la recolección de datos personales. → **“El diario y sus tarjetas”**
- Seguridad de los datos personales contra acceso y divulgación no autorizados.
- Derechos individuales: acceso, rectificación, limitación, borrado y portabilidad de datos.
- Notificación a autoridades y partes afectadas en caso de filtraciones de datos.
- Criterios legales para transferencias transfronterizas de datos.
- DPO (Delegado de Protección de Datos) monitorea el cumplimiento y asiste a las autoridades.
- **Cumplimiento Efectivo:**
 - Previene problemas legales, daños a la reputación y pérdida de confianza.
 - Políticas sólidas de protección de datos.
 - Principio de privacidad desde el diseño (Privacy-by-design).
 - Evaluaciones de impacto en la privacidad.
 - Capacitación a empleados. → **No implica fidelidad...**
 - Revisión y actualización continua de procesos de protección de datos.

Gestión de Riesgos - Ambientales

- Leyes creadas por gobiernos para garantizar la seguridad pública, reducir la contaminación y promover prácticas responsables con el medio ambiente.
- Protegen el entorno de actividades humanas y fomentan el uso sostenible de recursos naturales.
- Reducen contaminantes y el cambio climático.
- Residuos, agua, aire, uso del suelo, biodiversidad y cambio climático.
- Protegen ecosistemas, vida silvestre y recursos naturales.
- **Prevención y Control de la Contaminación:**
 - Tecnología más limpia, controles de emisión y gestión de residuos.
- **Conservación de Recursos:**
 - Apoyan la gestión sostenible, la eficiencia de recursos y la conservación.
 - Minimizan las emisiones de gases de efecto invernadero, aumentan la eficiencia energética y facilitan el cambio a energías bajas en carbono y renovables.

Gestión de Riesgos – Herramientas regulación

- Evaluaciones de Impacto Ambiental (EIA).
- Permisos y requisitos de cumplimiento para empresas e industrias.
- Medidas de control de la contaminación.
- Sistemas de gestión ambiental (EMS).
- Mecanismos de aplicación.
- Participación de las partes interesadas.
- Cooperación internacional.
- **Cumplimiento Efectivo:**
 - Evita problemas legales y daños a la marca para las empresas.
 - Sistemas de gestión ambiental sólidos.
 - Auditorías periódicas. → ¿ACUMAR?
 - Prevención de la contaminación.
 - Actualización constante sobre cambios regulatorios.
- **Beneficios del Cumplimiento:**
 - Aumentan la competitividad, el cumplimiento y la sostenibilidad ambiental.

Gestión de Riesgos – Específicas por Industria

- **Importancia:**
 - Abordan peligros, desafíos y preocupaciones específicas de cada industria.
 - Garantizan el funcionamiento adecuado y la seguridad.
 - Regulan las operaciones corporativas y establecen estándares dentro de la industria.
- **Obligación de Cumplimiento:**
 - Incumplimiento puede resultar en sanciones legales, multas, daño a la reputación y dificultades operativas.
 - Las organizaciones deben conocer las regulaciones de su industria.
 - Implementar sistemas de cumplimiento sólidos.
 - Realizar auditorías frecuentes.
 - Verificar el cumplimiento de sus actividades.
- **Objetivos:**
 - Consideran los problemas y oportunidades específicas de cada industria.
 - Seguridad, bienestar público, calidad de productos y servicios, competencia justa y abierta, protección del medio ambiente.
- **Beneficios del Cumplimiento:**
 - Funcionamiento legal, protección de marca y crecimiento a largo plazo.
 - Enfrentar problemas específicos del sector y promover prácticas comerciales éticas.

Gestión de Riesgos - Operacionales

- Surgen de las actividades habituales de un negocio.
- Relacionados con factores internos y externos que pueden afectar las metas de la empresa.
- **Impacto:**
 - Pérdidas monetarias, daño a la reputación, violaciones regulatorias e interrupciones en la empresa.
- **Gestión de Riesgos:**
 - Identificar, evaluar y mitigar los riesgos operacionales para un funcionamiento eficiente.
 - Reduce la ineficiencia, el daño a la credibilidad y las pérdidas monetarias.
- **Adaptación Continua:**
 - Revisión, modificación y mejora del proceso para mantenerse actualizado ante el cambiante entorno empresarial y los riesgos asociados.



Gestión de Riesgos – Cadena abastecimiento

- Eventos o circunstancias inesperados que interrumpen el flujo continuo de bienes, servicios o información dentro de una red de cadena de suministro.
- Desastres naturales, factores políticos, problemas con proveedores, variabilidad en la demanda o amenazas de ciberseguridad.
- Retrasos en la producción, aumento de costos, insatisfacción del cliente y daño a la reputación.
- **Estrategias de Gestión:**
 - Realizar evaluaciones de riesgo → Desarrollar planes de contingencia.
 - Diversificar proveedores para reducir la dependencia de una única fuente. → Scoring de proveedores vs Socios estratégicos
 - Gestión eficaz del inventario (ej. mantener stock de seguridad).
 - Colaboración y comunicación con proveedores y socios comerciales.
- **Resiliencia de la Cadena de Suministro:**
 - Planificación de continuidad del negocio: identificar proveedores alternativos, establecer instalaciones de respaldo, implementar medidas de contingencia
 - Redundancia, flexibilidad y agilidad para navegar por las interrupciones y mantener las operaciones.
- **Beneficios de la Gestión Proactiva:**
 - Minimizar el impacto de las interrupciones → Garantizar la continuidad del negocio.
 - Cumplir con las expectativas del cliente. → Mantener una ventaja competitiva.
- **Clave para el Éxito:**
 - Monitoreo, evaluación y adaptación constantes para gestionar eficazmente las interrupciones y mantener una red de cadena de suministro sólida y resistente.

Gestión de Riesgos – Fallas IT

- Interrupciones o averías en sistemas e infraestructura tecnológica que impactan negativamente las operaciones del negocio.
- **Causas:**
 - Fallas de hardware o software, ataques cibernéticos, errores humanos o desastres naturales.
- **Impacto:**
 - Pérdidas financieras, interrupciones operativas, pérdida de seguridad de datos y daño a la reputación.
- **Estrategias de Gestión:**
 - Evaluaciones de riesgo para identificar vulnerabilidades e implementar medidas preventivas.
 - Soluciones de respaldo y recuperación (copias de seguridad fuera del sitio y planes de recuperación ante desastres) para garantizar la disponibilidad e integridad de los datos.
 - Medidas sólidas de ciberseguridad (firewalls, antivirus, capacitación a empleados) para proteger contra amenazas cibernéticas.
- **Marco de Gestión Efectiva:**
 - Establecer marcos de gobierno de TI adecuados y cumplir con las regulaciones y estándares para un control efectivo de los sistemas informáticos.
 - Planes de respuesta a incidentes y estrategias de continuidad del negocio para garantizar acciones rápidas y coordinadas durante fallas informáticas.
- **Mantenimiento y Prevención:**
 - Actividades de monitoreo y mantenimiento regulares, y programas de capacitación y concientización para empleados para detectar problemas de manera temprana y promover prácticas informáticas responsables.
- **Beneficios de la Gestión Proactiva:**
 - Minimizar el riesgo de fallas informáticas y su impacto en las operaciones comerciales.
 - Medidas proactivas, respuesta efectiva a incidentes y prácticas sólidas de ciberseguridad para sistemas informáticos confiables y seguros, permitiendo operaciones comerciales fluidas y salvaguardando datos críticos.

Gestión de Riesgos - Procesos

- Deterioro o ineficiencia en un proceso empresarial, impactando negativamente el rendimiento y la satisfacción del cliente.
- **Causas:**
 - Diseño inadecuado del proceso. / Limitaciones de recursos. / Fallas de comunicación.
 - Capacitación insuficiente.
 - Deficiente monitoreo del desempeño.
- **Estrategias de Gestión:**
 - Analizar y mapear el proceso para identificar cuellos de botella y áreas de mejora. → Rediseñar el proceso para eliminar actividades sin valor agregado y agilizar flujos de trabajo.
 - **Asignar recursos suficientes para respaldar la ejecución fluida del proceso.**
 - Establecer canales y protocolos de comunicación efectivos para minimizar malentendidos y mejorar la coordinación.
 - Brindar programas de capacitación integrales para dotar a los empleados de las habilidades y conocimientos necesarios para la ejecución del proceso.
 - Implementar métricas de desempeño y mecanismos de monitoreo para rastrear el desempeño del proceso e identificar áreas de preocupación.
 - **Crear una cultura de mejora continua fomentando que el personal descubra fallas en el proceso y proponga soluciones.**
- **Beneficios de la Gestión Efectiva:**
 - Mejorar la eficiencia operativa, la productividad y la satisfacción del cliente.
 - Revisión periódica, rediseño, mejora del proceso y asignación adecuada de recursos y comunicación para la optimización del proceso.
 - Una cultura de mejora continua y participación de los empleados asegura el éxito sostenido en la gestión y mejora de los procesos.

Gestión de Riesgos – Error humano

- Actos u omisiones cometidas por empleados que se desvían del resultado deseado o esperado.
- Legalmente: **Acción, Inacción u omisión**
- **Causas:**
 - **Falta de preparación o experiencia / Fatiga mental o física. / Distracciones externas. / Exceso de confianza.**
- **Impacto:**
 - Riesgos de seguridad comprometidos / Pérdida de producción. / Aumento de gastos. / Daño a la reputación.
- **Estrategias de Gestión:**
 - Capacitación y formación integral para mejorar el conocimiento, las habilidades y la conciencia de los empleados sobre situaciones potenciales de error.
 - Estandarizar procedimientos para minimizar la ambigüedad y la probabilidad de errores.
 - Crear un entorno de trabajo que reduzca las distracciones e interrupciones.
 - Utilizar automatización y tecnología para minimizar el error humano.
- **Cultura de Aprendizaje:**
 - Fomentar que los empleados informen errores o cuasi accidentes sin temor a sanciones, permitiendo el análisis y la mejora.
 - Comunicación y trabajo en equipo efectivos para reducir malentendidos y errores.
- **Mejora Continua:**
 - Revisar incidentes o errores, identificar las causas raíz e implementar acciones correctivas.
- **Objetivo:**
 - Si bien el error humano no se puede eliminar por completo, las organizaciones pueden tomar medidas proactivas para mitigar su ocurrencia e impacto.

Gestión de Riesgos - Mercado

- Las variaciones en el precio del mercado pueden afectar el éxito financiero y la estabilidad de una organización.
- **Riesgo de Tasa de Interés:**
 - Los cambios en las tasas de interés pueden afectar las finanzas de una organización.
 - Las tasas de interés afectan los costos de endeudamiento, el rendimiento de las inversiones y los valores de renta fija.
 - El aumento de las tasas de interés podría elevar los pagos de intereses y los costos de financiamiento si una empresa tiene deuda a tasa variable.
 - Los swaps de tasa de interés, las herramientas de cobertura y la diversificación de la cartera de deuda pueden reducir el riesgo de tasa de interés.
- **Riesgo de Tipo de Cambio:**
 - Los tipos de cambio de divisas se modifican, especialmente cuando una empresa opera en varias monedas.
 - Los tipos de cambio afectan los activos, pasivos, ingresos y gastos en moneda extranjera.
 - Una devaluación de la moneda local podría reducir el valor de las ganancias en moneda extranjera para una empresa que vende productos en el exterior.
 - Las organizaciones pueden cubrir el riesgo cambiario mediante derivados de divisas o cobertura natural.
- **Riesgo de Precio de los Commodities:**
 - Una organización está expuesta a variaciones en el precio de los commodities, como petróleo, gas, metales, productos agrícolas y otros recursos básicos.
 - Las empresas que utilizan commodities o están expuestas a los mercados de commodities pueden sufrir volatilidad en los costos o ingresos.

Gestión de Riesgos – Crediticios

- Afecta a empresas que otorgan crédito a consumidores, invierten en títulos de deuda o negocian con contrapartes.
- Surgen del incumplimiento financiero de las contrapartes.
- **Riesgo de Incumplimiento de la Contraparte:**
 - Riesgo de que una contraparte no cumpla con sus obligaciones financieras.
- **Riesgo de Concentración:**
 - Ocurre cuando una empresa tiene una exposición crediticia excesiva a un solo prestatario o un pequeño grupo de prestatarios.
- **Riesgo de Liquidez:**
 - Una empresa carece de efectivo o activos fácilmente convertibles para cumplir con sus obligaciones financieras a corto plazo.
 - Lo causan desajustes entre entradas y salidas de efectivo, fuentes de financiamiento a corto plazo, activos ilíquidos o la imposibilidad de acceder rápidamente al efectivo sin una pérdida considerable de valor.
 - Puede provocar problemas financieros o insolvencia.

Gestión de Riesgos – Delictivo / Impacto errores

- Inherentes a las operaciones diarias de cualquier organización e impactan significativamente su salud financiera, reputación y éxito general.

Dos tipos comunes incluyen:

- **Fraude:**

- Actos engañosos intencionales o tergiversaciones realizadas por individuos dentro o fuera de la organización para beneficio personal.
- Incluye malversación, robo, falsificación y manipulación de registros financieros.
- Puede dañar la marca, las finanzas, la posición legal y la confianza del cliente.
- Para reducir el riesgo de fraude, las organizaciones deben implementar segregación de funciones, monitoreo y auditorías regulares, sistemas de denuncia y capacitación en prevención y detección de fraude.

- **Errores de Procesamiento:**

- Ocurren cuando se cometen errores o inexactitudes durante los procesos operativos.
- La entrada de datos, el procesamiento de transacciones, la conciliación y las dificultades del sistema pueden causar estos errores.
- Pueden provocar pérdidas financieras, insatisfacción del cliente, problemas regulatorios y retrasos.
- La revisión doble de datos, la validación automatizada y la revisión de procedimientos operativos pueden reducir los errores de procesamiento.
- Invertir en sistemas y tecnología confiable también puede ayudar.

Gestión de Riesgos - Reputacional

- Amenaza la marca, imagen o impresión pública de una organización.
 - Causas: Prensa negativa, percepción pública de actividad poco ética, malas experiencias del cliente o cualquier evento que empañe la credibilidad y confianza de la organización.
 - Impacto: Pérdida de consumidores, cuota de mercado, talento, atención legal y regulatoria, y daño a la marca.
- **Redes Sociales y Reputación Online:**
 - Las organizaciones pueden interactuar con su audiencia y dar forma a su reputación a través de las redes sociales y las plataformas online.
 - Conllevan riesgos intrínsecos que pueden afectar la reputación de una organización.
- **Importancia de la Gestión:** El mundo digital actual exige la gestión de redes sociales y reputación. → NO ES un simple “community manager” → Tiene que saber
- **Riesgos en Redes Sociales:** Las publicaciones en redes sociales pueden volverse virales en minutos, tanto buenas como malas.
 - Las organizaciones se enfrentan a riesgos de reputación porque no pueden controlar lo que la gente dice de ellas.
 - La información negativa o inexacta se propaga rápidamente, lo que dificulta la corrección o eliminación.

Gestión de Riesgos – Reputación on line

- Monitoreo regular de las redes sociales y la reputación online para mantenerse actualizado sobre las menciones de la marca.
- Responder rápida y abiertamente a las quejas y problemas de los consumidores demuestra dedicación a su satisfacción.
- Crear una estrategia de contenido que se alinee con los objetivos y valores de la empresa para impulsar la imagen de marca.
- La gestión de influencers (stakeholders) mejora la reputación de marca y el mensaje positivo.
- Tener un plan de gestión de crisis para redes sociales y reputación online para manejar comentarios y problemas negativos.
- Capacitar a los empleados sobre las mejores prácticas y normas de las redes sociales para garantizar que sus acciones online reflejen los valores de la empresa y no dañen su reputación.
- Las reseñas online, tanto positivas como negativas, dan forma a la percepción pública.
- **Beneficios de la Gestión:**
 - La gestión de redes sociales y reputación online puede reducir los riesgos reputacionales e impulsar la imagen de marca.
 - **Claves para el Éxito en la Era Digital: Responder, ser honesto y ser proactivo en las conversaciones y comentarios online permite a las empresas mantener una buena presencia y reputación online.**

Gestión de Riesgos – Media Management

- Impacto: La publicidad positiva puede mejorar la reputación al destacar los éxitos, mientras que la cobertura negativa puede destruirla a través de escándalos o controversias.
- Gestión de la Cobertura Mediática: Las relaciones públicas proactivas, la planificación de la comunicación en crisis y la monitorización online ayudan a gestionar la cobertura mediática.
- **Estrategias para una Cobertura Positiva:**
 - Comunicados de prensa, entrevistas y asociaciones pueden impulsar la cobertura mediática. Aumenta el conocimiento de la marca, la credibilidad y la confianza.
 - Relación con los Medios: Las organizaciones deben interactuar con los periodistas, proporcionar información confiable y contribuir a las conversaciones de la industria.
- **Manejo de Crisis:**
 - La cobertura mediática negativa requiere un plan de comunicación de crisis. Resolver el problema, entregar información correcta y tomar las medidas adecuadas es crucial. La comunicación reduce el daño y restaura la confianza.
- **Relaciones Públicas:**
 - La gestión de la reputación requiere buenas conexiones con los medios. Las relaciones, los intereses de los periodistas y la información oportuna son cruciales. Las relaciones públicas controlan la cobertura y garantizan una representación positiva.
- **Monitorización de Medios:**
 - La monitorización de medios ayuda a identificar riesgos, responder preguntas y corregir errores.
 - Es fundamental monitorear y participar en las redes sociales y las plataformas de internet.
 - Responder a comentarios y unirse a conversaciones da forma a la percepción pública y mantiene una presencia online favorable.

Gestión de Riesgos – Stakeholders (todos)

- La reputación y el éxito de una organización dependen de las relaciones con los stakeholders.
- Importancia: Es crucial generar confianza, lograr objetivos y alcanzar la sostenibilidad a largo plazo con los stakeholders.
- **Gestión Efectiva:**
 - Priorizar a los stakeholders clave según su impacto e importancia para gestionar eficazmente las interacciones.
 - Comunicación Continua: El contacto regular con los stakeholders promueve la transparencia y los informa sobre las acciones de la organización.
- **Alineación de Intereses:**
 - Alinear los intereses de los stakeholders con los objetivos de la organización crea interacciones beneficiosas para todos.
 - Colaboración: La colaboración y la cooperación permiten a las partes compartir conocimientos y puntos de vista, dando como resultado soluciones beneficiosas para todos.
- **Recopilación de Perspectivas:**
 - Las encuestas a stakeholders, los grupos focales y los diálogos directos revelan sus perspectivas y expectativas. La retroalimentación ayuda en la toma de decisiones y la mejora.
- **Sostenibilidad y Apoyo Comunitario:**
 - La sostenibilidad y el apoyo comunitario impulsan la reputación de una organización y las relaciones con los stakeholders.
- **Evaluación y Adaptación:**
 - La evaluación de los stakeholders ayuda a las empresas a adaptarse a la dinámica cambiante de estos grupos.
 - La flexibilidad y la capacidad de adaptación son clave para mantener relaciones sólidas.

Gestión de Riesgos – Evaluación de riesgos

- Proceso de detectar, analizar y valorar las posibles amenazas a los objetivos de una organización.
 - Incluye identificar riesgos, analizar su probabilidad y evaluar su impacto.
 - La evaluación de riesgos ayuda a fundamentar la toma de decisiones y la mitigación de riesgos.
- **Evaluación del Riesgo: Impacto vs. Probabilidad**
- La evaluación del riesgo implica valorar la importancia de los riesgos considerando su impacto potencial y la probabilidad de ocurrencia.
 - **Impacto:** La severidad posible de un evento de riesgo.
 - **Probabilidad:** La posibilidad de que ocurra el riesgo.
- Al evaluar el impacto y la probabilidad, las organizaciones DEBEN priorizar y asignar recursos para gestionar los riesgos.

Gestión de Riesgos – Impacto

- El impacto de un riesgo afecta los objetivos, operaciones y grupos de interés de una organización.
- Puede variar según el contexto específico y la naturaleza del riesgo.
- Los riesgos financieros, de mercado y de reputación operativa pueden afectar la rentabilidad, la imagen de marca y los procesos comerciales.
- La evaluación del impacto incluye pérdidas financieras, interrupciones operativas, daños a la reputación, ramificaciones legales y regulatorias, y peligros para la seguridad.
- Dependiendo de los datos y el riesgo, el impacto puede ser cuantificado o medido en un aspecto cualitativo.

Gestión de Riesgos - Probabilidad

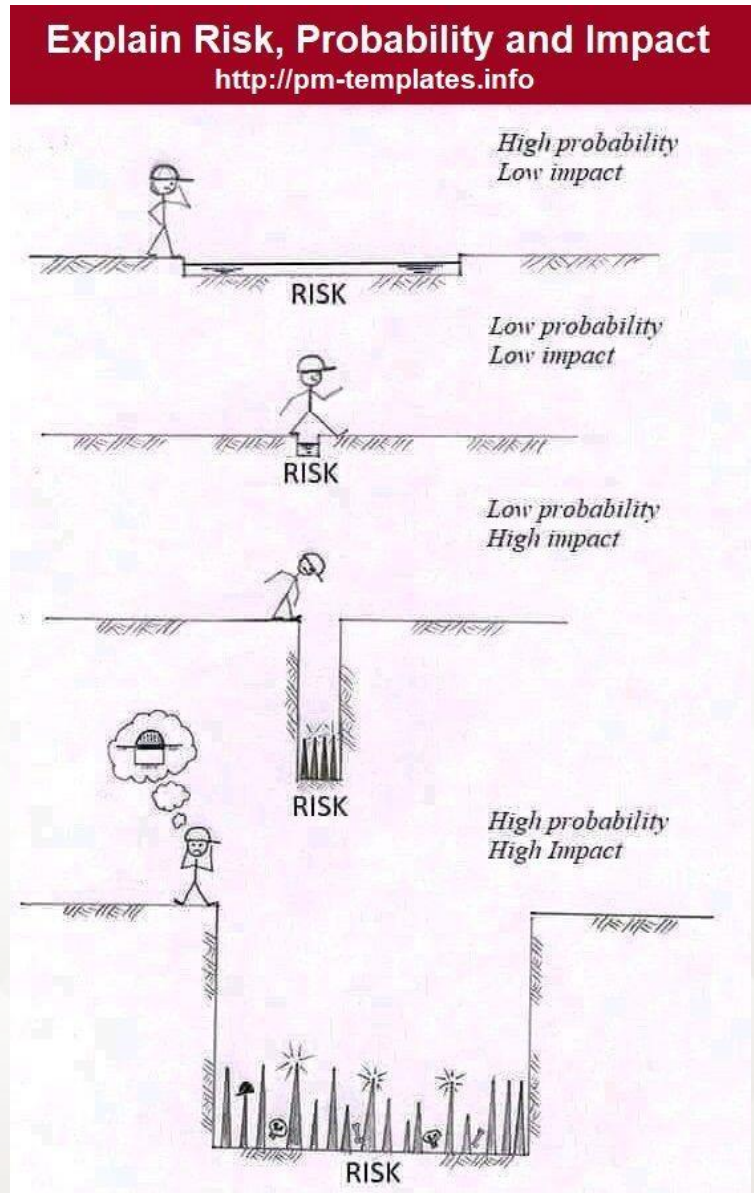
- Posibilidad de que ocurra un evento de riesgo.
- Se trata de evaluar la frecuencia o probabilidad del evento de riesgo dentro de un plazo determinado.
- La probabilidad se puede evaluar utilizando datos históricos, puntos de referencia de la industria, evaluación de expertos o análisis estadísticos.
- Las organizaciones pueden predecir riesgos evaluando la probabilidad.
- Los riesgos pueden tener una probabilidad baja, media o alta según la posibilidad de ocurrencia.
- “Hasta el pelo más delgado hace sombra en el suelo” → Martín Fierro

Gestión de Riesgos – Priorizar riesgos

- La evaluación del riesgo debe considerar el impacto y la probabilidad. Esto mejora la evaluación del riesgo y su importancia.
- Los riesgos de alto impacto y alta probabilidad se priorizan porque amenazan a la organización y necesitan una respuesta rápida.
- Estos riesgos pueden necesitar mitigación proactiva del riesgo, preparación para contingencias o transferencia del riesgo.
 - Por otro lado, los riesgos con bajo impacto y baja probabilidad pueden considerarse menos críticos y puede que no requieran una acción inmediata.
- Estos riesgos pueden cambiar con el tiempo, por lo que deben ser monitoreados y reevaluados.
- **Beneficios de la Evaluación de Riesgo:**
 - El impacto y la probabilidad ayudan a las empresas a priorizar la gestión de riesgos y asignar recursos.
 - Este enfoque prioriza los riesgos que podrían dañar o interrumpir los objetivos de la organización.
 - También ayuda a las empresas a detectar riesgos de baja probabilidad pero de alto impacto.

Gestión de Riesgos

- No existe el riesgo cero...
- Las matrices de riesgo pueden NO ser adecuadas para todas las organizaciones
- El esquema Red-Amber-Green no considera:
 - Criticidad Sinérgica
 - Estacionalidad
 - Destreza del “realizador” de la tarea



Check point

Gestión de Riesgos – Tolerancia y Aceptación

- **Tolerancia al Riesgo:** Es el nivel de riesgo que una empresa está dispuesta a aceptar o soportar para lograr sus objetivos. Influyen la cultura organizacional, la fortaleza financiera, la legislación y las expectativas de las partes interesadas.
- **Apetito al Riesgo:** Representa la actitud general de la organización frente al riesgo y la cantidad de riesgo que está dispuesta a aceptar → **cumplir sus objetivos. → Quien no piensa cumplir no pone reparo en las condiciones**
- **Alineación:** Crucial para una gestión de riesgos efectiva.
 - La tolerancia al riesgo debe estar alineada con el apetito al riesgo para garantizar la coherencia en la toma de decisiones.
 - Las organizaciones con un mayor apetito al riesgo pueden tener una mayor tolerancia al riesgo, lo que les permite adoptar estrategias más agresivas y aceptar mayores niveles de riesgo.
 - Por el contrario, las organizaciones con un apetito al riesgo conservador pueden tener una menor tolerancia al riesgo, priorizando la evitación o mitigación del riesgo.
- **Revisión y Reevaluación:** Necesarias para adaptarse a las circunstancias cambiantes.
- **Beneficios de Definir Tolerancia y Apetito al Riesgo:**
 - Tomar decisiones informadas, asignar recursos de manera efectiva y desarrollar estrategias de gestión de riesgos que respalden los objetivos mientras se gestionan los riesgos dentro de límites aceptables.
 - **Importancia:** Entender y gestionar la tolerancia al riesgo y el apetito al riesgo permite a las organizaciones encontrar un equilibrio entre la toma de riesgos y la mitigación del riesgo, **garantizando que naveguen por las incertidumbres de una manera alineada con sus objetivos estratégicos y capacidades de gestión de riesgos.**

Gestión de Riesgos - Técnicas

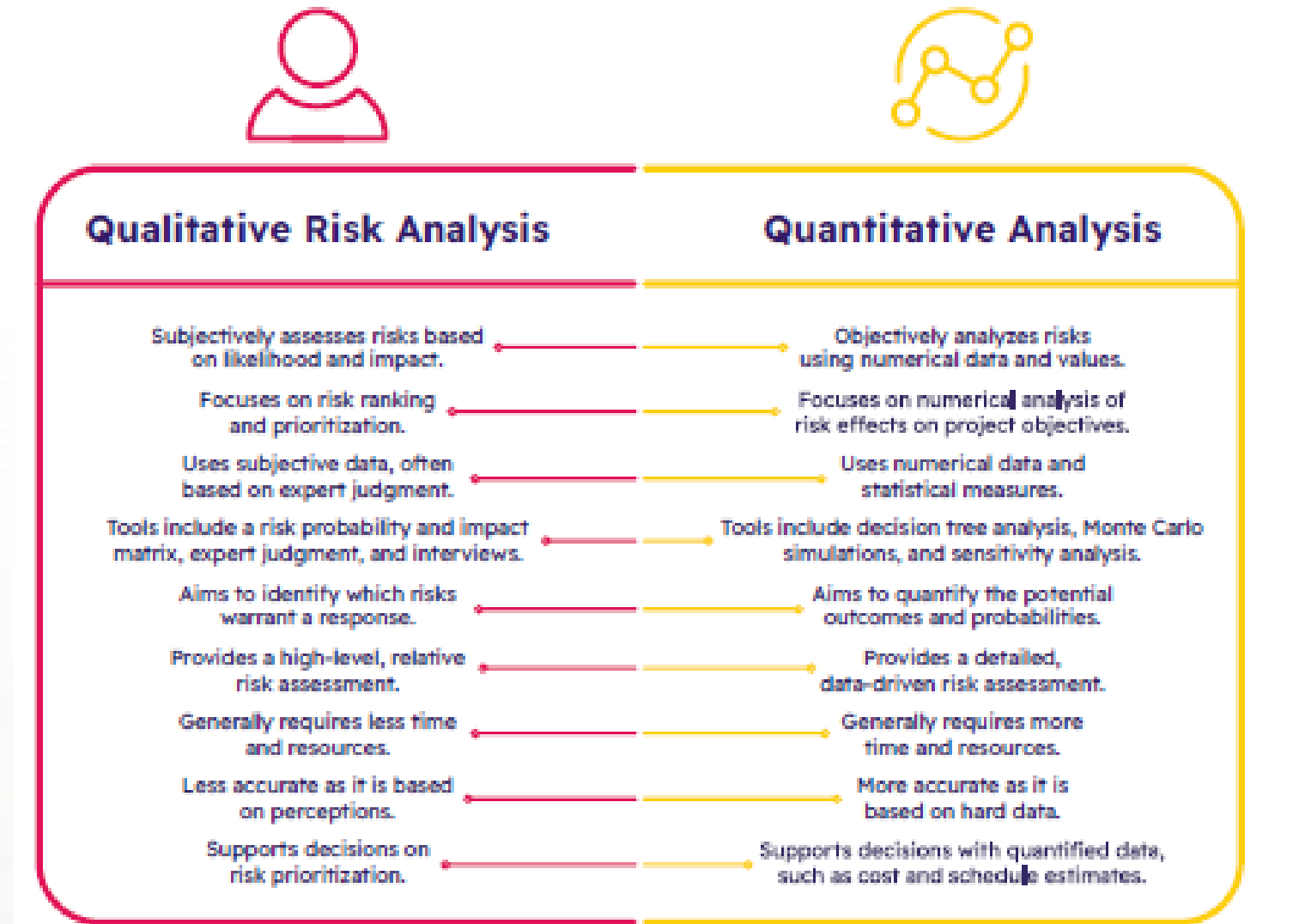
- Parte integral de la gestión de riesgos ya que ayudan a las empresas a prepararse y responder ante eventos que puedan poner en peligro sus objetivos.
 - **Brainstorming:** Actividad grupal cuyo objetivo es generar la mayor cantidad posible de ideas y amenazas diferentes. Beneficia el proceso de identificación al fomentar la creatividad, la transparencia y la inclusión de otros puntos de vista.
 - **Análisis FODA (Fortalezas, Oportunidades, Debilidades, Amenazas):** Examina las oportunidades y peligros que enfrenta una empresa, así como sus fortalezas y debilidades internas.
 - **Análisis de Escenarios:** Permite examinar cómo diferentes tipos de incertidumbre podrían afectar a una organización → Para prever y prepararse para futuros problemas → cómo prepararse para una “amplia gama” de futuros y los peligros asociados a cada uno.
- **Beneficios:** Proporcionan a las empresas una forma metódica de identificar potenciales peligros.
- **Implementación Efectiva:** Las empresas deben emplear estas técnicas de manera rutinaria e incluir a las partes interesadas clave para establecer un proceso integral de identificación de riesgos.
 - Mejorar su capacidad de recuperación y sus posibilidades de éxito.

Gestión de Riesgos - Análisis

- Examinar riesgos potenciales para determinar su **severidad, frecuencia y exposición**.
- Analizar su importancia relativa ayuda a identificar las amenazas más urgentes.
- **El análisis de riesgos permite tomar decisiones informadas sobre técnicas de gestión de riesgos y asignación de recursos.**
- **Análisis Cualitativo de Riesgos:**
 - Técnica subjetiva que analiza y evalúa riesgos según sus características cualitativas. Implica detectar y categorizar riesgos, analizar su impacto y probabilidad posibles, y clasificarlos por importancia.
 - Esta estrategia es útil cuando hay datos limitados o cualitativos, y ayuda a las empresas a comprender la naturaleza de los riesgos y tomar decisiones informadas sobre su gestión.
- **Proceso:**
 - Evaluar riesgos usando escalas o categorías descriptivas para severidad de consecuencias y probabilidad de ocurrencia.
 - Considerar factores como fuente del riesgo, áreas o procesos afectados, y naturaleza de las consecuencias.
 - Analizar cualitativamente los riesgos para entender sus posibles repercusiones, probabilidad de ocurrencia, velocidad de aparición, detectabilidad y vínculos con otros riesgos.
- **Resultados:**
 - La evaluación de riesgos considera el perfil de riesgo general y la tolerancia al riesgo de la organización.
 - Luego, se priorizan los riesgos para enfocarse en aquellos que requieren atención y mitigación inmediata.
- **Beneficios:**
 - El análisis cualitativo de riesgos ofrece a las empresas una visión subjetiva de los riesgos, permitiéndoles construir estrategias de gestión de riesgos que aborden las preocupaciones identificadas.
 - Es importante destacar que, de ser posible, la investigación cualitativa debe complementarse con análisis cuantitativo para una evaluación de riesgos más completa.
- **Ventajas:**
 - Las organizaciones pueden obtener información valiosa sobre la naturaleza y magnitud de los riesgos.
 - Permite asignar recursos de manera eficiente, establecer técnicas adecuadas de tratamiento de riesgos y tomar decisiones informadas para gestionarlos dentro de su tolerancia al riesgo.

Gestión de Riesgos

- El eterno dilema de valorar... y llevar a dinero lo intangible...
- Cualitativo **O** Cuantitativo...
- En realidad, es Cualitativo **Y** Cuantitativo...



Gestión de Riesgos – Matriz Probabilidad/Impacto

- También llamada matriz de riesgos o mapa de calor de riesgos.
- Herramienta gráfica para clasificar riesgos según su severidad e impacto posibles.
- La representación gráfica ayuda a las partes interesadas a comprender la gravedad de la situación de un vistazo.
- Cuadrícula con celdas que reflejan el impacto del riesgo y la probabilidad de ocurrencia.
 - Eje de probabilidad (de menor a mayor): raro, improbable, posible, probable, casi seguro.
 - Eje de impacto (de menor a mayor): insignificante, menor, moderado, sustancial, severo.
- La severidad del riesgo se visualiza según su ubicación en la matriz.
- **Priorización:**
 - Amenazas de alta probabilidad-alto impacto requieren atención y mitigación inmediatas.
 - Amenazas de menor prioridad (baja probabilidad-bajo impacto) requieren menos acciones urgentes.
- **Beneficios:**
 - Ayuda a la gestión de riesgos al permitir comparar y priorizar riesgos según su ubicación en la matriz.
 - Facilita la comunicación entre interesados al mostrar los riesgos visualmente.
 - Ayuda en la toma de decisiones, asignación de recursos y gestión de riesgos.
- **Limitaciones:**
 - Se basa en juicios subjetivos y comprime los riesgos en dos dimensiones, lo que puede no reflejar su complejidad.

Gestión de Riesgos

- No todos los riesgos deben (ni pueden) ser ponderados de la misma forma
- Pero... es simple de entender...
- La clasificación suele ser ajustada para los organismos de contralor...

Probability and Impact Matrix

		IMPACT				
PROBABILITY		Trivial	Minor	Moderate	Major	Extreme
	Rare	Low	Low	Low	Medium	Medium
	Unlikely	Low	Low	Medium	Medium	Medium
	Moderate	Low	Medium	Medium	Medium	High
	Likely	Medium	Medium	Medium	High	High
	Very likely	Medium	Medium	High	High	High

<https://www.justgetpmp.com/>

Gestión de Riesgos – Juicio Experto

- Un recurso valioso en la gestión de riesgos, ya que ofrece perspectivas y consejos útiles.
- **Funciones:**
 - Identificar, analizar, mitigar, decidir y monitorear riesgos.
 - Detectar peligros que otros podrían pasar por alto gracias a su conocimiento específico del sector o profesión.
 - Proporcionar una imagen completa del riesgo al revelar peligros y sus fuentes.
 - Estimar la probabilidad, el impacto y la verosimilitud del riesgo basado en su experiencia.
 - Ayudar a las organizaciones a priorizar y distribuir recursos según las evaluaciones de riesgo.
- **Beneficios:**
 - Soluciones sólidas para la reducción de riesgos.
 - Su conocimiento permite sugerir controles, transferencias de riesgo y medidas de protección.
 - Asesoramiento para crear planes de mitigación de riesgos específicos para la organización.
 - Ofrecen diversos puntos de vista y analizan riesgos e impactos para una mejor toma de decisiones.
 - Su experiencia ayuda a los interesados a tomar mejores decisiones en situaciones difíciles o ambiguas.
- **Evaluación y Monitoreo:**
 - Evalúan riesgos, tendencias de la industria y cambios regulatorios durante el monitoreo y la evaluación.
 - Su conocimiento ayuda a las organizaciones a modificar los métodos de gestión de riesgos y evitar posibles peligros.
- **Limitaciones:**
 - Tiene limitaciones y sesgos → Cognitivos y subjetivos
 - Se recomienda incluir a múltiples especialistas y tener en cuenta diversas opiniones para reducir sesgos y garantizar una evaluación de riesgos equilibrada.
 - **No se es “experto” por haber trabajado en la industria → no se las “sabe todas”...**

Gestión de Riesgos – Calidad de datos

- Proceso que evalúa la corrección, integridad, relevancia y confiabilidad de los datos de riesgo.
- Incluye identificar y evaluar fuentes de datos, verificar exactitud e integridad, y garantizar relevancia y confiabilidad.
- **Proceso:**
 - **Selección de Fuentes:** Inicia con la selección de tipos y fuentes de datos apropiadas. Incluye fuentes externas como publicaciones de la industria, estadísticas de mercado e información regulatoria.
 - **Precisión:** Una vez identificadas las fuentes, la evaluación se centra en la veracidad de los datos. Busca discrepancias, anomalías y valores atípicos que puedan poner en duda la precisión de la evaluación de riesgos.
 - **Integridad:** También considera la integridad de los datos, verificando la ausencia de vacíos y la corrección de la información. Los vacíos de datos pueden afectar las estimaciones de riesgo, por lo que es vital llenarlos.
 - **Relevancia:** Se examina la relevancia de los datos para la gestión de riesgos. Se verifica que los datos cubran el período de tiempo, la amplitud geográfica y las clasificaciones de riesgo especificados. La relevancia de los datos hace que las evaluaciones de riesgos sean pertinentes y aplicables. → **Los adverbios**
 - **Confiabilidad:** La evaluación de la calidad de los datos incluye la confiabilidad. Implica evaluar la precisión de la información, considerando técnicas de recolección de datos, fuentes y procedimientos. Fuentes creíbles y sin sesgos proporcionan datos confiables. → Falacias ad hominem
 - **Documentación:** La evaluación debe incluir la identificación de fuentes de datos, suposiciones, limitaciones y transformaciones o manipulaciones. La documentación mejora la calidad y transparencia de los datos.
- **Beneficios:**
 - La evaluación revela las fortalezas y debilidades de los datos de gestión de riesgos.
 - Identifica problemas de calidad de los datos, incluida la recolección y el gobierno de los datos.
 - **Una mejor calidad de los datos mejora el análisis de riesgos, la toma de decisiones y la gestión de riesgos en general.**

Gestión de Riesgos – Análisis Cuantitativo

- Proceso metódico que evalúa y cuantifica riesgos mediante herramientas numéricas y enfoques estadísticos.
- Asigna valores numéricos a características del riesgo como la probabilidad y el impacto, permitiendo una comprensión más objetiva y cuantificativa de los peligros.
- **Etapas:**
 - Analizar la exposición o vulnerabilidad a los riesgos.
 - Cuantificar las probabilidades de eventos de riesgo.
 - Evaluar el impacto potencial o las consecuencias de esos eventos.
 - Agregar riesgos para evaluar el perfil de riesgo general.
 - Evaluar los resultados para tomar decisiones informadas.
- **Beneficios:**
 - Las empresas pueden priorizar y asignar recursos mejor al evaluar la probabilidad y la gravedad probable de las amenazas.
 - Permite comparar y evaluar objetivamente diversos riesgos según estimaciones numéricas, facilitando una mejor toma de decisiones.
 - Ayuda a las empresas a determinar las pérdidas potenciales por riesgos específicos, útil para la prevención y planificación futura.
 - Presentar los riesgos en términos cuantificables facilita su discusión y comprensión.
- **Limitaciones:**
 - Depende de la disponibilidad y calidad de los datos, las estimaciones de probabilidad e impacto, y los supuestos del modelo.
 - **El benchmark puede no funcionar en todos los casos → a veces no existe → A veces no se puede acceder**
 - Puede haber aspectos cualitativos que el análisis numérico no capte por completo, así como incertidumbres y limitaciones relacionadas con el proceso de cuantificación.
 - Los resultados cuantitativos deben interpretarse a la luz de la información cualitativa y el juicio profesional.

Gestión de Riesgos – Análisis Sensibilidad

- Se realiza para evaluar cómo los cambios en las variables de entrada impactan los resultados de un modelo o estudio.
- Ayuda a los tomadores de decisiones a entender mejor cómo los cambios en las variables mencionadas influyen sus elecciones.
- Se eligen variables de entrada y se modifican dentro de un rango predeterminado o un conjunto de escenarios. Luego, se ejecuta el modelo o análisis para cada valor y se monitorea el efecto en la salida.
- El objetivo es aprender qué factores de entrada afectan más fuertemente la salida y cómo esos hallazgos cambian en respuesta a otras entradas.
- Ventajas:
 - Ayuda a determinar cuáles son los riesgos o incertidumbres más significativos para un determinado estudio.
 - Permite a los tomadores de decisiones gestionar y reducir los riesgos relacionados con los factores de entrada estudiando los efectos de esas variables en el resultado.
 - **Ayuda a tomar las mejores decisiones posibles en un mundo lleno de incógnitas. → Coin toss / Best of seven**
 - Los tomadores de decisiones pueden probar la estabilidad de sus juicios y sopesar los riesgos y beneficios de acciones alternativas.
 - Ayuda a la asignación de recursos al centrarse en los aspectos más influyentes.

Gestión de Riesgos – Valor Monetario Esperado

- El análisis de EMV es una técnica de análisis de riesgo cuantitativo que evalúa el impacto financiero probable de diferentes escenarios de riesgo.
- Se calcula la probabilidad de ocurrencia de cada riesgo y su valor monetario esperado.
- **El valor monetario esperado se obtiene multiplicando la probabilidad de un evento de riesgo por su costo monetario.**
- El análisis EMV brinda a los tomadores de decisiones información valiosa sobre las consecuencias financieras de distintos riesgos.
 - Permite priorizar la gestión de riesgos al asignar un valor monetario a sus potenciales consecuencias.
- Beneficios del análisis EMV:
 - Permite clasificar los riesgos según su potencial impacto financiero.
 - Ayuda a asignar recursos de manera efectiva enfocándose en los riesgos con mayor EMV.
 - Permite considerar las potenciales ganancias o pérdidas monetarias asociadas a diferentes opciones o cursos de acción.
- Limitaciones del análisis EMV:
 - La estimación precisa de la probabilidad e impacto monetario puede ser difícil debido a la subjetividad e incertidumbre.
 - El análisis EMV asume independencia entre las probabilidades y los valores monetarios, lo cual no siempre ocurre en la realidad.
- **Es importante complementar los resultados del EMV con elementos cualitativos, juicio de expertos y métodos analíticos alternativos.**

Gestión de Riesgos - Montecarlo

- Modelar y analizar sistemas o procesos inciertos.
- Genera muestras aleatorias para las variables de entrada dentro de rangos predeterminados.
- El modelo se ejecuta varias veces para determinar una variedad de resultados y su probabilidad asociada.
- Funciona definiendo primero las variables de entrada del sistema.
 - Estas variables tienen distribuciones de probabilidad que indican la probabilidad de valores distintos.
 - Se utilizan estas distribuciones para crear muestras aleatorias que el modelo usa para generar resultados.
 - Produce múltiples resultados al repetir este procedimiento cientos o millones de veces.
 - Analizar los resultados revela diferentes resultados y su probabilidad.
 - Esta metodología ayuda a los tomadores de decisiones en situaciones de incertidumbre a evaluar resultados y tomar decisiones informadas.
- Beneficios de la simulación Monte Carlo:
 - Permite ver todos los resultados posibles al explorar la incertidumbre de un sistema o proceso.
 - Ayuda a evaluar los riesgos y beneficios de diferentes opciones y estimar su probabilidad.
 - Favorece la toma de decisiones y la gestión de riesgos.
- Limitaciones de la simulación Monte Carlo:
 - La precisión y confiabilidad dependen de la calidad de los datos y las distribuciones de probabilidad.
 - Los modelos complejos requieren una gran cantidad de recursos de procesamiento y tiempo.
 - **Algunas organizaciones se basan SOLO en lo numérico**

Gestión de Riesgos – Eventos discretos

- Modelar y analizar sistemas o procesos complejos.
- Se identifican los componentes del sistema y sus interacciones se modelan como eventos con tiempos específicos.
- La simulación de eventos discretos involucra:
 - Modelar el sistema.
 - Programar eventos según su tiempo de ocurrencia y prioridad → Procesar cada evento para actualizar el estado del sistema.
- Corre hasta una condición de finalización preestablecida → analizan datos → rendimiento y tomar decisiones.
- Ventajas de la simulación de eventos discretos:
 - Modela sistemas complejos con interacciones discretas para examinar su comportamiento dinámico a lo largo del tiempo.
 - Permite a los tomadores de decisiones evaluar tácticas mediante la simulación de situaciones y políticas.
 - Identifica cuellos de botella, ineficiencias y oportunidades de mejora en el sistema.
 - Puede modelar el comportamiento del sistema en el tiempo.
 - Considera la secuencia de eventos para modelar con precisión procesos del mundo real.
 - Su capacidad para modelar tiempos y secuencias la hace valiosa en producción, logística, atención médica y transporte.
- Limitaciones de la simulación de eventos discretos:
 - Se necesita una comprensión completa del sistema y datos de entrada correctos para crear un modelo de simulación creíble.
 - **Los sistemas a gran escala requieren una construcción de modelos y formulación de programas de eventos con uso intensivo de computación. → pero no son “Big Data” → Volumen, Variedad y Velocidad**

Check point

Gestión de Riesgos - Mitigación

- Es el proceso de tomar medidas para reducir la gravedad y la frecuencia de posibles eventos adversos.
- Implica cualquier acción que disminuya la probabilidad de que suceda algo negativo a tu negocio, proyecto o proceso.
- Reducir los peligros potenciales ayuda a las personas y las empresas a mantenerse operando.



Gestión de Riesgos - Evitar

- Evitar por completo los peligros o encontrar otras formas de afrontarlos.
- Implica tomar decisiones para mantenerse alejado de acciones o circunstancias potencialmente peligrosas.
- De esta manera, las empresas pueden:
 - Reducir el impacto de cualquier resultado negativo → Protegerse de daños.
- Formas de implementar la evitación de riesgos:
 - **Selección de productos o servicios:** Las organizaciones eligen no ofrecer o utilizar productos o servicios con riesgos inherentes.
 - **Toma de decisiones estratégicas:** Se prioriza invertir en mercados, sectores o iniciativas de bajo riesgo.
 - **Contratos:** Se transfiere la responsabilidad y la carga de riesgos específicos a otras partes.
 - **Medidas de seguridad:** Se invierte en monitoreo, restricciones de acceso y prácticas seguras para evitar accidentes, brechas de seguridad e interrupciones operativas.
- Limitaciones de la evitación de riesgos:
 - Evitar riesgos puede significar perder oportunidades o limitar el progreso.
- Se deben sopesar los riesgos y las ventajas de la evitación del riesgo frente a los objetivos y la tolerancia al riesgo de la organización.

Gestión de Riesgos - Reducción

- Parte fundamental de la gestión de riesgos e implica tomar medidas preventivas para disminuir la probabilidad y el impacto de posibles peligros.
- Se analizan los peligros para determinar su probabilidad e impacto.
- Métodos de reducción de riesgos:
 - Mejoras de procesos / Avances tecnológicos / Cambios regulatorios / Programas de entrenamiento / Mejores prácticas de la industria
 - Monitoreo continuo: Se realiza para mantener la efectividad y relevancia de los mecanismos de control.
- **Métodos comunes de reducción de riesgos:**
 - Sistemas redundantes
 - Mantenimiento e inspecciones regulares
 - Mejoras en la ciberseguridad
 - Capacitación en conciencia de riesgos
 - Diversificación de proveedores
 - Planes de continuidad del negocio
- **Beneficios de la reducción de riesgos:**
 - Mejora la capacidad de recuperación y la protección de activos.
 - Ayuda a las empresas a anticipar y mitigar interrupciones, pérdidas financieras, daños a la reputación y otros problemas.
 - Contribuye a la estabilidad de la empresa.
- **Limitaciones de la reducción de riesgos:**
 - No elimina los riesgos por completo.
 - Es importante combinarla con otras técnicas de gestión de riesgos como la transferencia, aceptación y el compartir de riesgos.

Gestión de Riesgos – Riesgo Compartido

- **Compartir o transferir riesgos** a terceros, como compañías de seguros, socios contractuales o inversores, se conoce como "riesgo compartido" y es un método de gestión de riesgos.
- La idea es **poner en común recursos** para disminuir el impacto monetario y los resultados negativos de los riesgos.
- Las organizaciones pueden **reducir el impacto de eventos desfavorables** y mejorar su gestión de riesgos con la ayuda de este método.
 - **Técnicas de riesgo compartido:**
 - **Seguros:** Las organizaciones transfieren riesgos específicos a las compañías de seguros a cambio del pago de primas.
 - **Contratos y acuerdos:** Reparten la carga y aseguran la gestión de riesgos asignando riesgos y deberes a la parte adecuada.
 - **Empresas conjuntas y alianzas:** Permiten compartir recursos, experiencia y riesgos.
 - **Subcontratación:** Las empresas pueden externalizar tareas y la gestión de riesgos a proveedores externos.
 - **Inversión y financiamiento:** Se comparte el riesgo del proyecto y las pérdidas con inversores o prestamistas.
- **Beneficios del riesgo compartido:**
 - Reduce las responsabilidades financieras.
 - Mejora la capacidad de recuperación.
 - Brinda acceso a conocimientos y recursos externos.

Gestión de Riesgos - Aceptación

- La aceptación del riesgo es un método de gestión de riesgos en el que una organización decide **no tomar medidas preventivas** para enfrentar posibles consecuencias negativas.
- Implica reconocer un peligro y decidir que **vale la pena asumirlo** para lograr un objetivo.
- Es importante diferenciar la "aceptación del riesgo" de la "negligencia" o "ignorancia del riesgo". Estas últimas implican **falta de diligencia o imprudencia**.
- Las organizaciones aceptan riesgos por varias razones:
 - El análisis de costo-beneficio indica que **mitigar el riesgo es más caro** que la posible ocurrencia del mismo.
 - Aceptar el riesgo y destinar recursos a áreas prioritarias puede ser más rentable.
- Los peligros incontrolables también afectan la aceptación del riesgo.
 - Desastres naturales o eventos geopolíticos suelen estar fuera del control de una organización.
 - Aceptar estos riesgos implica reconocer los límites de la prevención y la mitigación, centrándose en gestionar sus posibles consecuencias.
- El apetito de riesgo (la disposición de una organización a asumir riesgos para lograr sus objetivos) también influye en la aceptación del riesgo. El sector industrial, la cultura y los objetivos estratégicos determinan el apetito de riesgo.
- Además, la aceptación del riesgo puede ser parte de una estrategia más amplia de **diversificación del riesgo**.
 - Las organizaciones pueden reducir el riesgo aceptando algunos riesgos en un área.
 - La diversificación disminuye la exposición de la empresa a riesgos individuales.
- La aceptación del riesgo requiere evaluaciones de riesgo exhaustivas, evaluación de posibles repercusiones y estándares y procesos claros para la toma de decisiones. → **Documentación y sign-off**

Gestión de Riesgos – Monitoreo y Reporte

- La gestión eficaz de riesgos requiere una atención constante y reportes sobre el estado de los peligros potenciales.
- El monitoreo de riesgos implica seguirlos de cerca de manera organizada a medida que avanzan por diversas etapas.
 - Objetivos:
 - Identificar riesgos emergentes o posibles dificultades que puedan dañar los objetivos de la organización.
 - Detectar cambios en el panorama de riesgos.
 - Evaluar la eficacia de los controles de riesgo.
- **Métodos para el monitoreo de riesgos:**
 - Evaluaciones de riesgo.
 - Monitoreo de indicadores clave de riesgo.
 - Análisis de incidentes.
 - Revisiones de controles internos.
 - Uso de tecnología y soluciones automatizadas para simplificar el proceso y obtener datos en tiempo real.
- **El reporte de riesgos implica la comunicación de información relacionada con el riesgo a las partes interesadas:**
 - Gerencia. / Junta directiva. / Empleados. / Partes externas (reguladores e inversores).
- **Objetivos del reporte de riesgos:**
 - Brindar a las partes interesadas una visión profunda del perfil de riesgo de la empresa.
 - Presentar las exposiciones al riesgo actuales.
 - Informar sobre cambios importantes o nuevos peligros que necesitan ser abordados.

Gestión de Riesgos – Reporte de riesgos

- Información presentada de manera concisa y comprensible.
- Mediciones de riesgo, tendencias y análisis.
- Descripción narrativa de los riesgos clave y su posible impacto en la empresa.
- **Beneficios del monitoreo y reporte continuo de riesgos:**
 - Fomenta la comunicación abierta, la responsabilidad y la toma de decisiones informadas en todos los niveles.
 - Permite a la gerencia identificar y clasificar las amenazas para asignar recursos y desarrollar contramedidas.
 - Ayuda a las partes interesadas a comprender el apetito de riesgo de la empresa, las iniciativas de gestión de riesgos y sus posibles efectos en el desempeño y la reputación.
- **Factores para mejorar el monitoreo y reporte de riesgos:**
 - Roles y responsabilidades claras para la supervisión de riesgos.
 - Canales de comunicación efectivos. → **Denuncias anónimas**
 - Información de riesgo precisa, confiable y actualizada.
 - Revisión y actualización de métodos para adaptarse a cambios en el panorama de riesgos y el entorno empresarial.
- **Importancia del monitoreo y reporte de riesgos:**
 - Permiten a las organizaciones mejorar la toma de decisiones, garantizar la responsabilidad y responder rápidamente a nuevos riesgos.
 - Fomentan una cultura consciente del riesgo, transparente y resiliente.

Gestión de Riesgos - Frameworks

- Las organizaciones pueden beneficiarse de un enfoque más sistemático para la gestión de riesgos utilizando **marcos de gestión de riesgos**.
- Estos marcos brindan pautas que las organizaciones pueden seguir para desarrollar un enfoque coherente y metódico para la gestión de riesgos.
- Un buen marco de gestión de riesgos permite a una empresa identificar y analizar las amenazas a sus activos, operaciones y reputación.
- También puede ayudar a la empresa a diseñar medidas de mitigación de riesgos, monitorear y reportar los niveles de riesgo, y aumentar la madurez de la gestión de riesgos.
- Existen varios marcos de gestión de riesgos ampliamente reconocidos utilizados por organizaciones a nivel mundial.
- **Todos forman parte del Compliance**

Gestión de Riesgos – ISO 31000

- Ayuda a las empresas a identificar, analizar, tratar y monitorear riesgos de manera estandarizada e integrada.
- Enfatiza la integración de la gestión de riesgos en el gobierno y la toma de decisiones.
- Promueve la creación de un marco de gestión de riesgos con políticas, objetivos y responsabilidades.
- Garantiza la gestión de riesgos en toda la organización.
- Recomendando evaluar factores internos y externos e incluir a las partes interesadas en la gestión de riesgos.
- Recomendando un enfoque sistemático e iterativo de la gestión de riesgos, con etapas como:
 - Establecimiento del contexto. / Identificación del riesgo. / Evaluación del riesgo. / Tratamiento del riesgo. / Monitoreo.
- Enfatiza la necesidad de evaluar los riesgos tanto cualitativa como cuantitativamente.
- Orienta a las organizaciones en la selección e implementación de opciones adecuadas de tratamiento del riesgo:
 - Evitación. / Transferencia. / Mitigación. / Aceptación.
- Destaca el monitoreo y la revisión continua del proceso de gestión de riesgos.
- Permite aprender de la experiencia, evaluar la efectividad de los controles de riesgo y realizar mejoras necesarias.
- **Beneficios de implementar ISO 31000:**
 - Mejora las prácticas de gestión de riesgos.
 - Fomenta una cultura consciente del riesgo.
 - Alinea los esfuerzos con las mejores prácticas reconocidas internacionalmente.
 - Proporciona un lenguaje y marco común para gestionar riesgos de manera efectiva.
 - Permite tomar decisiones informadas y mejorar el rendimiento general.

Gestión de Riesgos - Marco COSO (Committee of Sponsoring Organizations)

- Es el estándar de oro en la gestión de riesgos corporativos.
- Consta de ocho componentes interrelacionados que mejoran la capacidad de una organización para identificar, analizar, responder y monitorear riesgos.
- **Componentes:**
 1. **Ambiente interno:** Promueve una cultura consciente del riesgo y respalda una gestión de riesgos efectiva.
 2. **Establecimiento de objetivos:** Define objetivos claros considerando riesgos y oportunidades.
 3. **Identificación de eventos:** Reconoce eventos potenciales que pueden afectar el logro de objetivos.
 4. **Evaluación del riesgo:** Analiza la probabilidad e impacto de los riesgos identificados.
 5. **Respuesta al riesgo:** Desarrolla estrategias para abordar los riesgos identificados.
 6. **Actividades de control:** Implementa acciones para mitigar riesgos y asegurar objetivos.
 7. **Información y comunicación:** Facilita el flujo oportuno y relevante de información sobre riesgos dentro de la organización.
 8. **Monitoreo continuo:** Permite rastrear cambios en el perfil de riesgo, evaluar la efectividad de las respuestas y garantizar el funcionamiento del marco.
- **Beneficios:**
 - Mejora las prácticas de gestión de riesgos.
 - Alinea la gestión de riesgos con la toma de decisiones estratégicas.
 - Refuerza los controles internos.
 - Permite la identificación y respuesta proactiva a los riesgos.
 - Aumenta la capacidad para lograr objetivos, mitigar amenazas y aprovechar oportunidades.
 - Fomenta una cultura consciente del riesgo.
 - Mejora el rendimiento general y la capacidad de recuperación de la organización.

Gestión de Riesgos – Acuerdos de Basilea (Banks)

- Creados para salvaguardar las instituciones financieras globales.
- Objetivos:
 - Garantizar que los bancos tengan suficiente capital para absorber pérdidas y mantener la estabilidad financiera (función principal).
 - Establecer estándares globales para nivelar el campo de juego para los bancos.
 - Fortalecer la gestión del riesgo bancario, la transparencia y la disciplina de mercado.
- Basilea I (1988):
 - Se centró en el riesgo crediticio.
 - Definió un requisito mínimo de capital para los bancos basado en el riesgo ponderado de los activos.
 - Buscaba asegurar que los bancos tuvieran suficiente capital para soportar pérdidas.
- Basilea II (2004):
 - Buscó hacer que los requisitos de capital fueran más sensibles al riesgo.
 - Estableció requisitos mínimos de capital, revisión supervisora y disciplina de mercado.
 - Promovió los sistemas internos de gestión de riesgos de los bancos, métodos avanzados de medición de riesgos y requisitos de capital por riesgo operacional.
- Basilea III (post crisis financiera 2008):
 - Aumentó la regulación bancaria.
 - Elevó las regulaciones de capital y liquidez para fortalecer a los bancos durante las crisis financieras.
 - También limitó el apalancamiento y abordó el riesgo de crédito de contraparte, el riesgo de tasa de interés y los requisitos de transparencia.
- Crítica:
 - No abordan las vulnerabilidades relacionadas con las crisis financieras, incluido el riesgo de liquidez y la interconexión.

Gestión de Riesgos - NIST

- Marco de Gestión de Riesgos NIST (<https://www.nist.gov/cyberframework>)
- Enfoque sistemático y organizado para la gestión de riesgos en seguridad de la información y ciberseguridad.
- Guía a las empresas a través del proceso de identificar, evaluar y mitigar riesgos en sus sistemas de información.
- Etapas del NIST:
 1. **Categorización:** Identificar y clasificar los sistemas de información según su importancia e impacto potencial.
 2. **Selección:** Elegir controles de seguridad adecuados del catálogo NIST.
 3. **Implementación:** Despliegue real de los controles seleccionados.
 4. **Evaluación:** Efectividad de los controles mediante evaluaciones y pruebas de seguridad.
 5. **Autorización:** Revisión por la gerencia y toma de decisiones sobre la operación de los sistemas en base al riesgo residual.
 6. **Monitoreo:** Evaluación continua de los controles de seguridad para identificar nuevos riesgos o vulnerabilidades.
- Beneficios del NIST:
 - Gestión eficaz de los riesgos asociados a los sistemas de información.
 - Mejora de la postura general de seguridad.
 - Enfoque proactivo a la gestión de riesgos.
 - Integración de controles de seguridad en el ciclo de vida del desarrollo del sistema.
 - Protección de la información sensible.
 - Respuesta a amenazas emergentes.
 - Cumplimiento de requisitos regulatorios.
 - Establecimiento de una base sólida para gestionar los riesgos de ciberseguridad.
 - Protección continua de activos y datos críticos.

Gestión de Riesgos – Típicos por industria

- **Finanzas y Banca:**

- Enfrentan riesgos crediticios, de mercado, de liquidez y operativos.
- Esta industria utiliza análisis rigurosos, pruebas de estrés y cumplimiento normativo para analizar y mitigar riesgos.

- **Salud:**

- Los riesgos incluyen seguridad del paciente, errores médicos, cumplimiento normativo y privacidad de datos.
- La gestión de riesgos en salud abarca prácticas de seguridad del paciente, gestión de riesgos legales y regulatorios, y seguridad de datos.

- **Manufactura:**

- Sufre interrupciones en la cadena de suministro, dificultades en la calidad del producto, mal funcionamiento de equipos y seguridad del trabajador.
- La gestión de riesgos en manufactura incluye control de calidad, eficiencia en la cadena de suministro y seguridad.

- **Energía y Servicios Públicos:**

- Enfrentan la volatilidad de precios, el cumplimiento normativo, el impacto ambiental y las fallas en la infraestructura.
- Esta industria gestiona los riesgos del precio de la energía, las leyes ambientales y el mantenimiento preventivo.

Gestión de Riesgos

- **Construcción:**

- Sufre retrasos, sobrecostos financieros, problemas de seguridad y sanciones legales.
- La gestión de riesgos en construcción incluye planificación de proyectos, evaluaciones de riesgos, medidas de seguridad y gestión de contratos para reducir riesgos y asegurar el éxito del proyecto.

- **Venta Minorista y Bienes de Consumo:**

- Enfrentan interrupciones en la cadena de suministro, retiros de productos, pérdida de reputación de marca y violaciones de datos. La gestión de riesgos minorista incluye optimización de la cadena de suministro, control de calidad, gestión de marca y seguridad de datos.

- **Transporte y Logística:**

- Enfrentan accidentes, robos de carga, cumplimiento normativo e interrupciones en la cadena de suministro.
- La gestión de riesgos en este sector incluye capacitación de conductores, mantenimiento de vehículos, seguridad, legislación sobre transporte y planificación de contingencias ante disrupciones.

Gestión de Riesgos – Riesgos IT

- La gestión de riesgos informáticos implica detectar, analizar y mitigar los riesgos asociados a los sistemas, infraestructura y operaciones de TI de una empresa.
- Se trata de identificar amenazas y vulnerabilidades que puedan poner en peligro la confidencialidad, integridad y disponibilidad de los activos informáticos, y tomar medidas para mitigarlas.
- El objetivo principal es comprender las vulnerabilidades y amenazas a la confidencialidad, integridad y disponibilidad de los activos informáticos, y desarrollar métodos para mitigar los riesgos.
 - **Análisis de Riesgos:**
 - Una vez identificados los riesgos, se analizan para determinar su probabilidad e impacto potencial.
 - Esto incluye analizar la probabilidad del riesgo y su impacto en los sistemas de TI, datos y operaciones de la organización.
 - El análisis prioriza los riesgos y asigna recursos.
 - **Valoración de Riesgos:**
 - La valoración de riesgos determina la tolerancia al riesgo de la organización y qué riesgos necesitan una acción rápida.
 - Incluye comparar los riesgos medidos con los umbrales de riesgo.
 - Los riesgos que superan el umbral de riesgo de la organización deben tratarse de inmediato.
- **Tratamiento de Riesgos:**
 - Se desarrollan estrategias de tratamiento de riesgos para mitigar y gestionar los riesgos identificados.
 - Se pueden utilizar medidas de seguridad, resiliencia del sistema, capacitación del personal y planes de respuesta a incidentes.
 - El objetivo es reducir los riesgos y garantizar que la organización pueda responder y recuperarse de posibles incidentes.
- **Documentación y Reportes:**
 - La evaluación de riesgos informáticos requiere documentación y generación de informes.
 - La documentación del proceso asegura la transparencia y facilita la comunicación interna.
 - La documentación cubre los peligros, análisis, estrategias de tratamiento de riesgos y riesgos residuales después de la mitigación.
 - Los informes sobre el estado del riesgo de TI y la efectividad de la mitigación del riesgo ayudan a las partes interesadas a tomar decisiones informadas y administrar recursos.

Gestión de Riesgos – Medidas Seguridad

- Las organizaciones deben implementar medidas de seguridad para proteger sus datos, sistemas informáticos, confidencialidad, integridad y disponibilidad. Los pasos clave en el proceso de implementación son:
 - **Políticas y procedimientos de seguridad:** Proporcionan lineamientos y mejores prácticas para los empleados.
 - **Controles de acceso:** Autenticación fuerte y restricciones de acceso basadas en roles para proteger sistemas y datos.
 - **Seguridad de red:** Firewalls, IDPS y VPNs para proteger la red de la empresa.
 - **Protección de datos:** Medidas para salvaguardar la confidencialidad, integridad y disponibilidad de la información.
 - **Concientización y capacitación en seguridad:** Educar a los empleados sobre prácticas seguras y cómo detectar amenazas.
 - **Planes de respuesta a incidentes:** Estrategias para identificar, contener y recuperarse de incidentes de seguridad.
 - **Monitorización y auditoría de seguridad:** Detectar y responder a riesgos mediante la supervisión de sistemas y actividades.
 - **Gestión de la seguridad de proveedores y terceros:** Garantizar que los procesos de seguridad de los proveedores cumplen con los estándares de la organización.
 - **Cumplimiento normativo:** Implementar controles necesarios para cumplir con las regulaciones de la industria.
 - **Evaluaciones y actualizaciones periódicas de seguridad:** Identificar vulnerabilidades y mantener actualizados los sistemas y software.

Gestión de Riesgos – Auditoría IT

- Las organizaciones necesitan auditorías regulares de TI para evaluar el rendimiento y la seguridad del sistema.
- Estas auditorías examinan la infraestructura de TI, los controles y el cumplimiento normativo de la empresa.
- **Alcance de las Auditorías Regulares de TI:**
 - **Verificación de cumplimiento:** Verificar el cumplimiento de leyes, regulaciones y estándares de la industria.
 - **Evaluación de riesgos:** Identificar posibles amenazas a las operaciones y la seguridad de datos de la empresa. Esta evaluación prioriza la mejora y la minimización de riesgos.
 - **Evaluación de controles:** Evaluar la eficacia de los controles de TI existentes implementados por la organización. Se evalúan controles de acceso, gestión de cambios, planes de respuesta a incidentes y otras medidas de protección de activos de TI y continuidad del negocio.
 - **Revisión de sistemas y procesos:** Verificar la infraestructura de TI, software, redes y bases de datos para una configuración, mantenimiento y monitoreo correctos. También evalúa los procedimientos de TI.
 - **Seguridad e integridad de datos:** Analizar el cifrado de datos, restricciones de acceso, copias de seguridad, parches y actualizaciones de seguridad para proteger los datos confidenciales del acceso ilegal, la manipulación y la pérdida.
 - **Gobierno de TI:** Garantizar que las actividades de TI apoyen los objetivos comerciales y tengan roles y responsabilidades claras.
 - **Preparación para la respuesta a incidentes:** Evaluar las estrategias de respuesta a incidentes, la gestión y los sistemas de respaldo y recuperación.
 - **Beneficios de las Auditorías Regulares de TI:**
 - **Informe de auditoría detallado:** Resume hallazgos, deficiencias y sugerencias. Este estudio ayuda a realizar mejoras y optimizar los sistemas y controles de TI.
 - **Caso: 147 páginas**

Gestión de Riesgos – Respuesta incidentes

- La planificación de respuesta a incidentes es fundamental para la gestión de riesgos y la ciberseguridad.
- Implica planificar y ejecutar una estrategia organizada para eventos e interrupciones de seguridad.
- **Preparación:**
 - Identificar amenazas potenciales.
 - Formar equipos de respuesta a incidentes. / Definir roles y responsabilidades dentro del equipo.
 - Evaluar riesgos y vulnerabilidades para guiar las tácticas de respuesta.
- **Detección y Análisis:**
 - Monitorear sistemas y redes para detectar accesos ilegales o actividad anómala.
 - Investigar incidentes por parte del equipo de respuesta. / Decidir sobre una respuesta adecuada.
 - Recopilar evidencia para entender el incidente.
- **Respuesta:**
 - Aislar sistemas comprometidos para evitar propagación. / Asegurar la evidencia para posibles investigaciones legales.
 - Colaborar con las partes interesadas afectadas por el incidente.
 - Utilizar recursos externos si es necesario (ej. expertos forenses).
- **Mitigación y Recuperación: → ZERO DAY**
 - Eliminar malware u otros elementos dañinos.
 - Restaurar sistemas afectados a partir de copias de seguridad.
 - Implementar medidas de seguridad adicionales para prevenir futuros incidentes.
- **Beneficios de la Planificación de Respuesta a Incidentes: → HOT FIX**
 - Ayuda a las empresas a manejar incidentes de seguridad de manera efectiva.
 - Protege activos críticos de la organización.
 - Permite la continuidad de las operaciones durante y después de un incidente.

Gestión de Riesgos – En proyectos

- La gestión de riesgos de proyectos implica identificar, analizar y minimizar los riesgos que puedan afectar la finalización del proyecto.
- Esto incluye un análisis sistemático de riesgos, desarrollo de estrategias, y monitoreo y control a lo largo de todo el ciclo de vida del proyecto.
- La gestión de riesgos de proyectos minimiza los efectos negativos de los riesgos en los objetivos del proyecto y maximiza su éxito.
- Hay oportunidades...
 - “nadie lo hace”...
 - “que nos puede pasar...”
 - “no le importamos a nadie...”

Gestión de Riesgos – Project Risks

- Implica identificar, analizar y evaluar los posibles riesgos que puedan afectar el éxito de un proyecto.
 - 1. Identificación de Riesgos:**
 1. Analizar el alcance del proyecto, las partes interesadas, los recursos y los impactos externos para identificar posibles peligros.
 2. Este proceso utiliza lluvia de ideas, entrevistas a expertos y documentación del proyecto.
 - 2. Análisis de Riesgos:**
 1. Analizar en detalle los riesgos identificados.
 2. Evaluar la probabilidad e impacto de cada riesgo en los objetivos del proyecto.
 3. Utilizar análisis cualitativo y cuantitativo para evaluar la gravedad y probabilidad del riesgo.
 - Análisis Cualitativo: Asigna valores basados en el juicio de expertos.
 - Análisis Cuantitativo: Utiliza datos históricos o herramientas estadísticas para evaluar los riesgos de manera más objetiva.
 - 3. Evaluación de Riesgos:**
 1. Priorizar los riesgos según su importancia.
 2. Esta fase clasifica los riesgos según su posible influencia en los objetivos del proyecto.
 3. La priorización permite a los gerentes de proyecto centrarse en los riesgos más graves.
 - 4. Planificación de la Respuesta a Riesgos:**
 1. Elegir métodos para evitar, mitigar, transferir o aceptar riesgos según cada uno.
 2. Las técnicas de respuesta a riesgos buscan minimizar los riesgos del proyecto y aumentar el éxito.
- **Beneficios:**
 - Ayuda a prever y prepararse para posibles problemas del proyecto.
 - Permite una mejor toma de decisiones al priorizar riesgos.
 - Aumenta las probabilidades de éxito del proyecto.

Gestión de Riesgos – Planificar la respuesta

- La planificación de la respuesta a riesgos implica establecer formas de abordar los peligros del proyecto.
- La gestión de riesgos busca limitar los efectos negativos y capitalizar las oportunidades.

1. Evasión del Riesgo:

1. Eliminar o evitar por completo los peligros del proyecto.
2. Se utiliza cuando el impacto potencial de un riesgo excede la tolerancia del proyecto.
3. Al evitar riesgos, el equipo del proyecto puede reducir su impacto negativo.

2. Mitigación del Riesgo:

1. Reducir la probabilidad e impacto de un riesgo.
2. Medidas preventivas, planes de contingencia y mejoras de procesos ayudan a minimizar el riesgo y sus consecuencias.
3. Las medidas de mitigación reducen la gravedad de los peligros.

3. Transferencia del Riesgo:

1. Transferir la responsabilidad de un riesgo a un tercero.
2. Se logra mediante contratos, seguros o subcontratación.
3. Este método se utiliza cuando transferir el riesgo a una parte más capacitada es más beneficioso.
4. Si el riesgo se materializa, la transferencia del riesgo reduce los efectos financieros y operativos del proyecto.

Gestión de Riesgos – Planificar la contingencia

- La planificación de contingencia aborda de manera proactiva los riesgos e incertidumbres en un proyecto o negocio.
- **Proceso de Planificación de Contingencia:**
 - 1. Identificación de Riesgos e Incertidumbres:**
 1. Analizar posibles riesgos que puedan interrumpir el proyecto o negocio.
 2. Ejemplos: desastres naturales, fallas tecnológicas, interrupciones en la cadena de suministro, crisis económicas y cambios regulatorios.
 3. Comprender los riesgos ayuda al equipo del proyecto a prepararse.
 - 2. Desarrollo del Plan de Contingencia:**
 1. Crear planes para abordar cada riesgo identificado.
 2. Incluir acciones a tomar, roles de los miembros del equipo y recursos necesarios.
 3. El objetivo es mitigar riesgos y responder de manera efectiva.
 - 3. Componentes del Plan de Contingencia:**
 1. Reacción ante eventos de riesgo y recuperación de operaciones.
 2. Puede incluir sistemas de respaldo, cadenas de suministro alternativas, protocolos de comunicación y reasignación de recursos. → **What / When / Why / Where / Which / How**
 3. Considerar las implicaciones financieras, operacionales y de reputación en la mitigación de riesgos.
 - 4. Prueba y Actualización del Plan:**
 1. Realizar simulacros y ejercicios para identificar y corregir fallas en el plan.
 2. Aumenta la confianza del equipo y los prepara para enfrentar riesgos reales.

Gestión de Riesgos – Revisiones regulares

- Las revisiones regulares de proyectos permiten a los gerentes de proyecto y las partes interesadas medir el progreso y alcanzar los objetivos.
- **Seguimiento y Control del Proyecto:**
 - Analizar indicadores clave, hitos y entregables para evaluar el estado del proyecto y detectar desviaciones del plan.
 - Permite realizar ajustes y correcciones para mantener el proyecto en camino.
- **Mejora de la Comunicación:**
 - Fomentan la comunicación abierta entre el equipo del proyecto y las partes interesadas.
 - Permiten discutir problemas, intercambiar información y considerar opiniones diversas.
 - Las revisiones regulares promueven la solución colaborativa de problemas.
- **Identificación y Mitigación de Riesgos:**
 - Destacan riesgos y preocupaciones que podrían afectar los resultados.
 - Los datos del proyecto, los indicadores de rendimiento y las evaluaciones de riesgos ayudan a identificar y mitigar los peligros.
 - La gestión temprana de riesgos reduce los retrasos y fracasos del proyecto.
- **Participación de las Partes Interesadas:**
 - Permiten incorporar las opiniones y expectativas de las partes interesadas clave en el proceso de revisión.
 - **Aumenta la satisfacción y el apoyo de las partes interesadas.**
 - El compromiso de las partes interesadas fomenta la apropiación y la colaboración en el proyecto.

Check point

Evaluación y gestión de proyectos tecnológicos

- Una mirada profunda a las técnicas para evaluar el éxito o el fracaso
- La evaluación de la gestión de proyectos es un proceso crucial para **determinar la efectividad** con la que se ha gestionado un proyecto y si se han logrado los objetivos establecidos.
- Es un análisis sistemático que busca identificar áreas de éxito y áreas de mejora en la ejecución del proyecto.
- Si fracasa el proyecto
 - → Costo hundido
 - → irrecuperable
 - → ruedan cabezas...

Evaluación y gestión de proyectos tecnológicos

- **Mejorar el rendimiento futuro:** Al identificar las fortalezas y debilidades de la gestión del proyecto, las organizaciones pueden aprender de sus experiencias y mejorar su desempeño en futuros proyectos.
- **Aumentar la rendición de cuentas:** La evaluación proporciona evidencia del desempeño del equipo del proyecto y la gerencia, lo que fomenta la rendición de cuentas y la responsabilidad.
- **Promover la toma de decisiones informadas:** La información obtenida de la evaluación puede ayudar a los gerentes a tomar decisiones más informadas sobre la gestión de proyectos en el futuro.
- **Satisfacer las necesidades de las partes interesadas:** La evaluación puede ayudar a garantizar que se cumplan las expectativas de las partes interesadas y que el proyecto haya brindado valor.

Evaluación y gestión de proyectos tecnológicos

1. Establecer los objetivos de la evaluación:

1. El primer paso es definir los objetivos específicos de la evaluación, lo que ayudará a determinar el alcance y la metodología de la evaluación.

2. Identificar los criterios de evaluación:

1. Los criterios de evaluación deben estar alineados con los objetivos del proyecto y deben ser específicos, medibles, alcanzables, relevantes y con un plazo determinado (SMART).

3. Recopilar datos:

1. Los datos se pueden recopilar de diversas fuentes, como entrevistas, encuestas, revisión de documentos y observación.

4. Analizar datos:

1. Los datos recopilados se deben analizar para identificar patrones, tendencias y áreas de éxito o fracaso.

5. Preparar un informe de evaluación:

1. El informe de evaluación debe presentar los hallazgos de la evaluación, las conclusiones y las recomendaciones.

6. Compartir los resultados de la evaluación:

1. Los resultados de la evaluación deben compartirse con las partes interesadas relevantes para que puedan tomar medidas correctivas y mejorar el desempeño en futuros proyectos.

Evaluación y gestión de proyectos tecnológicos

- **Técnicas comunes para evaluar la gestión de proyectos**
 - **Análisis de las partes interesadas:**
 - Implica evaluar la satisfacción de las partes interesadas con el proyecto, incluyendo sus percepciones sobre la gestión del proyecto, la comunicación y el logro de los objetivos.
 - **Revisión de documentos:**
 - Revisar documentos del proyecto, como el plan del proyecto, los informes de estado, las actas de reuniones y la correspondencia, para evaluar la calidad de la planificación, la ejecución y el control del proyecto.
 - **Observación:**
 - Al equipo del proyecto en acción para evaluar sus habilidades, comportamientos y la dinámica del equipo.
 - **Encuestas:**
 - Se pueden utilizar para recopilar datos cuantitativos y cualitativos de las partes interesadas sobre su percepción de la gestión del proyecto. → puede que sea útil técnica Delphi
 - **Entrevistas:**
 - Recopilar datos en profundidad de las partes interesadas sobre sus experiencias y opiniones

Evaluación y gestión de proyectos tecnológicos

- **Consideraciones adicionales para la evaluación de la gestión de proyectos**
 - **La independencia del evaluador:**
 - El evaluador debe ser independiente del equipo del proyecto para garantizar la objetividad de la evaluación.
 - **La participación de las partes interesadas:**
 - Las partes interesadas relevantes deben participar en el proceso de evaluación para garantizar que sus perspectivas sean consideradas.
 - **El uso de métodos mixtos:**
 - La combinación de diferentes técnicas de evaluación puede proporcionar una visión más completa del desempeño de la gestión del proyecto.
 - **La ética de la evaluación:**
 - La evaluación debe realizarse de manera ética, respetando la confidencialidad de las partes interesadas y utilizando los datos recopilados de manera responsable.

Evaluación y gestión de proyectos tecnológicos

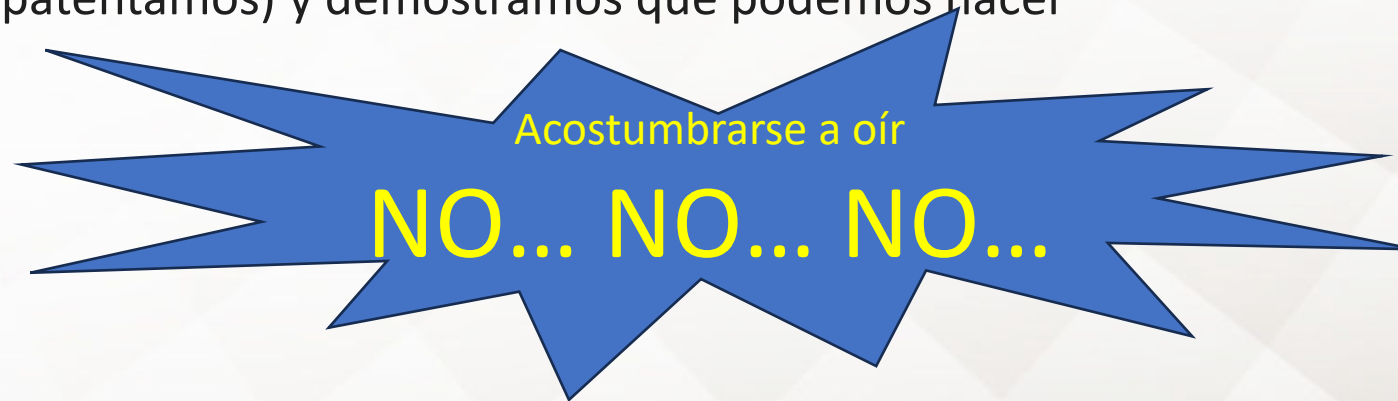
- ¿Conclusión? → Es solo el comienzo...
 - La evaluación de la gestión de proyectos es una herramienta valiosa para mejorar el desempeño de la gestión de proyectos y aumentar las posibilidades de éxito en futuros proyectos.
 - Al implementar un proceso de evaluación sistemático y riguroso, las organizaciones pueden identificar áreas de mejora, aprender de sus experiencias y tomar decisiones informadas para optimizar la gestión de sus proyectos.
 - El “experto” debe serlo, NO ÚNICAMENTE por sus años de vida...
 - No es un “side hustle” ni “gig work”...

Check point

Desarrollo de emprendimientos

Desarrollo de emprendimientos

- El mundo de las tecnologías de la información (TI) ofrece un terreno fértil para el surgimiento de **emprendimientos innovadores y disruptivos**.
- Si queremos emprender, debemos asegurarnos que :
 - Somos distintos... → ofrecemos lo mismo, pero de otra forma
 - Somos mejores... → que el statu quo existente en el “nicho”
 - Solucionamos un problema... → con un ratio costo/beneficio aceptable
 - Ofrecemos algo que falta...
 - → (primero lo patentamos) y demostramos qué podemos hacer



Desarrollo de emprendimientos

1. Identificar una necesidad real del mercado:

- **Problema o una necesidad real que los usuarios o clientes enfrentan.**
 - Esto implica
 - realizar una investigación de mercado exhaustiva
 - comprender las tendencias,
 - las necesidades insatisfechas
 - y las oportunidades existentes en el sector de TI.

2. Desarrollar una solución innovadora y diferenciada:

- Que aborde de manera efectiva.
 - Tu propuesta de valor debe destacarse de la competencia y ofrecer un beneficio tangible a los usuarios.
 - La innovación tecnológica puede/debe ser un factor clave para diferenciarte.
 - Inversores → Friends & Family → expandir al segundo círculo de conexiones → Networking
 - NO se usa más... pero... hacer tarjetas personales... → postales

Desarrollo de emprendimientos

3. Validar la viabilidad de tu idea:

- Crear un prototipo o una versión mínima viable de tu producto o servicio para probarlo con usuarios reales y obtener sus comentarios.
- Ayudará a identificar posibles problemas y a refinar la propuesta antes de lanzarla al mercado.

4. Armar un equipo talentoso y apasionado:

- El éxito de cualquier emprendimiento depende en gran medida de la calidad del equipo que lo impulsa.
- Rodearte de **personas talentosas, apasionadas por la tecnología y con las habilidades necesarias** para ejecutar tu plan de negocios será fundamental para alcanzar tus objetivos.
- No se buscan las personas ideales, se busca que idealmente, las personas trabajen potenciándose entre ellas. → Cultura → Historia → Tolerancia → Éxito

Desarrollo de emprendimientos

5. Desarrollar un modelo de negocio sólido:

- Generará ingresos y alcanzará la rentabilidad.
- Debe incluir aspectos como:
 - la estructura de precios,
 - los canales de distribución,
 - la estrategia de marketing
- y las proyecciones financieras. → “Me van a robar la idea” → HSBC **P** PSC

6. Adaptarse a los cambios y ser flexible:

- Dinamismo y constante evolución.
- Ser flexible y adaptable para poder responder a cambios del mercado, nuevas tecnologías y necesidades de los usuarios.
- La capacidad de “pivotar” y ajustar tu estrategia será crucial para el éxito a largo plazo.
 - → Be water my friend: Bruce Lee (<https://www.youtube.com/watch?v=MyQ8YzgqVdY>)

Desarrollo de emprendimientos

7. Proteger tu propiedad intelectual:

- Patentes, derechos de autor o marcas registradas.
 - → No lo hace “cualquier abogado”
- Asegurar tus activos y evitar que otros puedan “replicar o copiar” la idea.

8. Buscar financiamiento y apoyo:

- Cubrir los costos de desarrollo, lanzamiento y crecimiento. → Shark Tank
- Seed Capital / Angel Investors / Préstamos
- Buscar apoyo en incubadoras o aceleradoras de empresas que ofrecen asesoría, mentoría y acceso a redes de contactos.
- Networking... Casos
 - → HeliTaxi (2002)
 - → Ed-Gar → Ofishop → Staples + Office Depot (1996)

Desarrollo de emprendimientos

9. Construir una comunidad y generar engagement (compromiso):

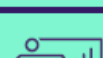
- Con los usuarios,
- obtener valiosos comentarios
- y construir una base de clientes leales.
- Las redes sociales, los eventos y el marketing de contenidos son herramientas útiles para conectar con tu audiencia. → Las galletitas variedades

10. Medir el rendimiento y tomar decisiones basadas en datos:

- Métricas clave y analizar los datos recopilados.
 - Identificar áreas de mejora.
 - Tomar decisiones informadas.
 - Optimizar tu estrategia de negocio.
- **11. El Equipo: “Nadie se salva solo”...**

Desarrollo de emprendimientos

- El equipo es fundamental
- ¿Cómo queremos liderar al equipo?
- No todos somos buenos en todo...
- Enfocarnos en las fortalezas de cada una de las personas.
- El talento natural debe ser “cultivado” → Invertir y tolerar el error → Dinero

 Performance Management	VS	 Performance Appraisal
This is a continuous, comprehensive process that involves setting objectives, performance planning, continuous monitoring and feedback, development, and performance reviews.	 DEFINITION	This is a subset of performance management, typically an annual process where a manager evaluates an employee's performance against set objectives and criteria.
Ongoing and continuous.	 TIME FRAME	Typically annual or semi-annual.
Looks at the future performance of employees, focusing on improvement, learning, and development. It is prospective.	 FOCUS	Primarily looks at the past performance of employees, assessing what has already occurred. It is retrospective.
Covers everything related to performance, including setting expectations, goal alignment, tracking progress, providing feedback, training, and development.	 SCOPE	Primarily focuses on evaluating an individual's performance, often linked to promotions or salary adjustments.
Continuous and regular feedback, coaching, and development.	 PROCESS	Periodic evaluation, typically a one-time event.
A proactive and strategic approach that aims at improving the future performance and potential of the employees.	 APPROACH	Often a reactive approach that assesses past performance.
Aims to enhance employee performance and align it with the organization's strategic goals.	 OUTCOME	Provides an evaluation that can be used for job feedback, promotions, or compensation decisions.

Desarrollo de Emprendimientos – El Equipo

- El método STAR es una técnica utilizada en las entrevistas de comportamiento para:
 - evaluar las habilidades
 - y la experiencia de un candidato
 - a través de ejemplos concretos.
- **S - Situación:** El entrevistador pedirá que describas una situación específica en la que te hayas enfrentado a un reto o desafío relacionado con el puesto que estás solicitando.
- **T - Tarea:** Explicar cuál era la tarea o responsabilidad en esa situación.
- **A - Acción:** Describir las acciones que tomaste para abordar la situación y el reto.
- **R - Resultado:** Explicar los resultados que obtuviste con tus acciones.

Check point

Carpeta de presentación

La carpeta de presentación

- Documento fundamental para ofrecer un proyecto de tecnologías de la información (TI).
- Comunicar de manera clara y concisa los detalles del proyecto, incluyendo: alcance, objetivos, metodología, beneficios esperados y costos asociados.
- **La estructura NO está tallada en piedra...**
- Si no puedo ir solo, voy acompañado..., si no puedo ser el Uno, puedo ser el Dos → Piluso y Coquito / Batman y Robin / Cerebro y Pinky / El Llanero y Toro
- Recordar:
 - La “regla” \$ 1 = \$ 1,50...
 - MoSCoW...
 - 80% uso...
 - +/- 3%-5% desvío tiempo / dinero... → A quién “le estoy vendiendo”...

La carpeta de presentación

1. Resumen ejecutivo

- Breve descripción del proyecto y sus objetivos principales.
- Problemática que se busca resolver o necesidad que se busca satisfacer.
- Propuesta de valor del proyecto para el cliente.
- Beneficios tangibles e intangibles esperados.

2. Descripción del proyecto

- Alcance del proyecto, incluyendo las funcionalidades, características y módulos que se desarrollarán.
- Metodología de trabajo que se utilizará para la ejecución del proyecto.
- Fases del proyecto y cronograma estimado para cada una de ellas.
- Recursos humanos y técnicos necesarios para llevar a cabo el proyecto.

La carpeta de presentación

3. Solución técnica

- Arquitectura tecnológica propuesta, incluyendo hardware, software, redes y plataformas.
- Descripción detallada de las tecnologías que se utilizarán en el proyecto.
- Justificación de la elección de las tecnologías seleccionadas.
- Consideraciones de seguridad y confiabilidad de la solución.

4. Análisis financiero

- Inversión inicial requerida para el proyecto.
- Costos recurrentes asociados al proyecto, como mantenimiento, soporte y licencias.
- Análisis de retorno de la inversión (ROI) del proyecto.
- Punto de equilibrio del proyecto.

La carpeta de presentación

5. Plan de gestión de riesgos

- Identificación de los principales riesgos asociados al proyecto.
- Plan de mitigación de riesgos para cada uno de los riesgos identificados.
- Responsable de la gestión de riesgos.

6. Conclusiones

- Resumen de los puntos clave del proyecto.
- Reiteración de los beneficios esperados para el cliente.
- Llamado a la acción para que el cliente tome una decisión sobre el proyecto.
- **NUNCA mentir... todos nos conocemos... y todos nos charlamos...**
- Qué incluir... “depende”... → **Double non disclosure con el cliente**

La carpeta de presentación

- Incluir:
 - Logo + Sitio Web + folletería + redes
 - En lo posible que sea fácil de pronunciar...
 - Debe ser profesional y atractiva. → **Canva PRO USD 6.90**
 - Utilizar un lenguaje claro y conciso, evitando tecnicismos excesivos.
 - → **Los números los van a ver contadores → Se complica el Total Cost of Ownership...**
 - Es importante utilizar gráficos, tablas y diagramas para ilustrar los puntos clave.
 - La carpeta DEBE adaptarse a las necesidades específicas del cliente. → A quién le vendo...
 - Investigar a fondo al cliente / negocio antes de preparar la carpeta de presentación.
 - La presentación del proyecto debe ser clara, concisa y convincente.
 - → Preparar el “30 seconds pitch” del proyecto y el personal
 - Se debe estar preparado para responder a las preguntas del cliente.

La carpeta de presentación

- Ejemplos para tomar ideas...
- <https://slidesgo.com/theme/information-technology-project-proposal>
- <https://blog.hubspot.com/agency/7-tips-presenting-winning-proposals-clients>
- <https://www.sba.gov/>

La carpeta de presentación

- **Medidas técnicas:**

- Indicadores de rendimiento clave (KPIs) que se utilizarán para medir el éxito del proyecto.
- Plan de pruebas para garantizar la calidad del software y la infraestructura.
- Plan de mantenimiento y soporte para la solución tecnológica.

- **Medidas económicas:**

- Análisis de sensibilidad del ROI del proyecto en diferentes escenarios económicos.
- Plan de financiamiento del proyecto, si es necesario.
- Estrategias para optimizar los costos del proyecto.

La carpeta de presentación

- **Medidas financieras:**

- ROI – ROI – ROI y luego...
- Cash-flow...
- Valor actual neto (VAN)
- Tasa interna de retorno (TIR) del proyecto.
- Payback period → Si lo hubiere...

- Cuanto “se pide” de anticipo al cliente

- 20% → 30%
- **Completion Bonus? → 23/04/2014 → un día (de) miércoles...**
- Pensar quién tiene leverage: ¿el cliente, el vendor o el partner?
- Tiers 1 / 2 / 3 → Conocernos...

Check point

Incubadoras tecnológicas

Incubadoras tecnológicas

- Espacios de apoyo y desarrollo para emprendimientos innovadores que buscan transformar el panorama digital.
 - Ofrecen un ecosistema integral que impulsa el crecimiento de startups con alto potencial en las áreas de software, hardware, internet de las cosas, inteligencia artificial, big data, Fintech y otras áreas de vanguardia tecnológica.
 - Sin ánimo de lucro o con fines de desarrollo social que brindan a los emprendedores de IT un conjunto de recursos, servicios y mentorías para que sus ideas se conviertan en negocios exitosos.
 - Catalizadores del “ecosistema emprendedor”, conectando a startups con expertos, inversores y potenciales clientes.
 - Entender el contrato de adhesión → **Tener nuestro abogado de confianza, que ENTIENDA del tema (somos pocos...)**

Incubadoras tecnológicas

- Proceso de selección riguroso para elegir a las start-ups que serán parte de su programa.
- Las seleccionadas reciben un apoyo integral que incluye:
 - **Espacio físico:** Las start-ups tienen acceso a un espacio de trabajo compartido o a oficinas privadas dentro de la incubadora, lo que les permite reducir costos y trabajar en un ambiente colaborativo.
 - **Asesoría y mentoría:** Los emprendedores reciben asesoría y mentoría personalizada por parte de expertos en diferentes áreas, como desarrollo de negocios, marketing, finanzas y aspectos legales.
 - **Capacitación y formación:** Se ofrecen talleres, cursos y seminarios para que los emprendedores adquieran las habilidades y conocimientos necesarios para gestionar su negocio.
 - **Acceso a redes de contactos:** Facilitan el contacto con inversores, potenciales clientes, socios estratégicos y otros actores relevantes del ecosistema emprendedor.
 - **Financiación:** Algunas incubadoras ofrecen programas de financiación o acceso a capital semilla para ayudar a las start-ups a despegar. → **Contador de confianza**

Incubadoras tecnológicas

Las start-ups que participan en programas de incubación obtienen numerosos beneficios, entre los que se destacan:

- **Aumento de las posibilidades de éxito:** La tasa de éxito de las start-ups que pasan por un programa de incubación es significativamente mayor que la de aquellas que no lo hacen.
- **Reducción del tiempo de desarrollo:** El apoyo y la orientación recibidos en la incubadora permiten a las start-ups acelerar su proceso de desarrollo y lanzamiento al mercado.
- **Acceso a recursos valiosos:** Las start-ups se benefician de una amplia gama de recursos, como espacios de trabajo, tecnología, asesoría legal y contable, y acceso a redes de contactos. → **A veces nos sugieren personas para nuestro equipo...**
- **Mayor visibilidad:** La participación en un programa de incubación aumenta la visibilidad de la start-up y la posiciona como una empresa innovadora y con alto potencial. → **Nos da respaldo cuando nos estamos formando un nombre...**

Incubadoras tecnológicas

- Las incubadoras tecnológicas están abiertas a **emprendedores con ideas innovadoras y disruptivas en el ámbito de las TI.**
- Las start-ups que postulan deben tener un **plan de negocios sólido, un equipo talentoso y comprometido, y un alto potencial de crecimiento.**
- **¿Cómo encontrar una incubadora tecnológica adecuada?**
 - Existen numerosas incubadoras tecnológicas en todo el mundo, cada una con sus propias características y enfoques.
 - Para encontrar la incubadora adecuada, es importante que los emprendedores **consideren aspectos como la especialización de la incubadora, el tipo de apoyo que ofrece, la red de contactos a la que da acceso, y los requisitos de selección.**
 - NETWORKING → NETWORKING → NETWORKING



Incubadoras tecnológicas

- Algunas conocidas:
 - Wayra (América Latina): <https://www.wayra.es/>
 - Plug and Play Tech Center (México): <https://www.plugandplaytechcenter.com/>
 - Startup Chile: <https://startupchile.org/en/>
 - Endeavor <https://endeavor-hub.com/>

Incubadoras tecnológicas

- Las incubadoras tecnológicas componente fundamental ecosistema IT
 - Apoyo y recursos a las start-ups con mayor potencial,
 - Contribuyen al desarrollo de la innovación tecnológica
 - y a la creación de nuevas empresas que impulsan el crecimiento económico y social.
- Idea innovadora en el ámbito de IT, → explorar las oportunidades que ofrecen las incubadoras tecnológicas no solo de nuestra región.
 - Apoyo adecuado,
 - Time to Market,
 - No es “suerte”... es perseverancia.

Check point

Índice

- Gestión de Riesgos
- Evaluación y Gestión de proyectos tecnológicos
- Desarrollo de Emprendimientos
- Incubadoras tecnológicas

¡Muchas Gracias!