DESARROLLO DE APLICACIONES DOJO.NET DIGITALGEKO

Prevención del Cibercrimen

- Existen varios mecanismos que nos apoyan en la prevención del Cibercrimen, entre estos están las “Alertas tempranas”, donde nuestras aplicaciones juegan un papel importante!

Recopilación de datos

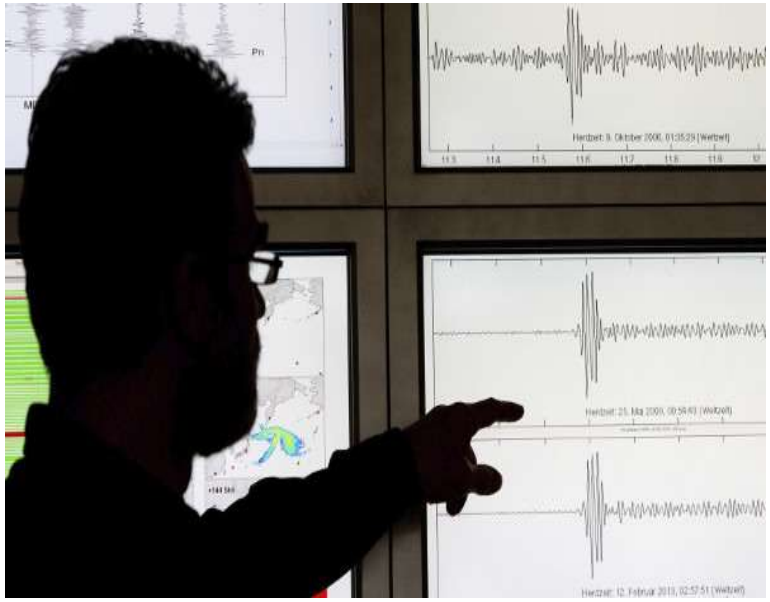
Los sistemas actualmente realizan diferentes transacciones y operaciones que facilitan a los operativos en sus tareas diarias. Es importante identificarlas y ponderar su nivel de riesgo de acuerdo a sus procesos.

Entre estas están:

- Contables
- Ingresos
- Pagos
- Transferencias
- Acceso a la información

Monitoreo de información

Los registros son generadores de información que sirven como base de análisis que permitan identificar actividades de riesgo que contribuyan a generar alertas a los equipos de **monitoreo y auditoria** para realizar validaciones y evitar que los eventos de Cibercrimen se materialicen.



“Nuestros sistemas diariamente realizan miles de transacciones importantes”.

Trazabilidad

La trazabilidad en sistemas se refiere a la capacidad de rastrear y relacionar elementos dentro de un sistema, desde su origen hasta su implementación, mantenimiento y operación. Esto permite entender cómo se conectan los requisitos, los componentes y las funciones en un sistema.

Tipos:

- **Trazabilidad hacia adelante**
- **Trazabilidad hacia atrás**
- **Trazabilidad bidireccional**

Propósito de la Trazabilidad

Control de calidad: Asegurar que todos los requisitos y operaciones se implementen correctamente.

Gestión del cambio: Evaluar el impacto de modificaciones en requisitos, componentes y datos.

Auditoría y cumplimiento: Demostrar que el sistema cumple con estándares y regulaciones.

Diagnóstico y mantenimiento: Identificar rápidamente fallos, intentos de ataque y sus causas.

Beneficios de la Trazabilidad

Reducción de riesgos: Mejora el control sobre errores y fallos.

Eficiencia: Minimiza el re-trabajo al facilitar el diagnóstico de problemas.

Cumplimiento normativo: Ayuda a cumplir con regulaciones internacionales.

MEDICIÒN DEL RIESGO

Registrar actividades de Riesgo

Base de datos centralizadas: Se recomienda utilizar una base de datos exclusiva para almacenar cada uno de los siguientes registros: Calidad, Monitoreo y para Riesgos.

Alertas y notificaciones: Implementar mecanismos de monitoreo que generen alertas en tiempo real cuando se detecten anomalías en los procesos.

Análisis Predictivo: Esta información generada se utiliza con herramientas sofisticadas para el análisis predictivo o la IA.

Equipo de Monitoreo: Desarrolla protocolos claros, guías de uso y equipo capacitado en las herramientas para evitar inconsistencias.

Actividades de Riesgo

Riesgos de crédito: Adquirir créditos sin un análisis adecuado. Otorgar los proyectos a proveedores que incumplan.

Riesgos de mercado: El riesgo asociado a las fluctuaciones en el valor de los activos y cambios en tasas en el mercado en caso de operaciones de Deuda Pública o colocación de Bonos.

Riesgo Operativo: Se refiere a perdidas por fallas en los procesos internos, errores humanos, fraudes internos o fallos tecnológicos.

- **Errores en la gestión de Transacciones** (pagos duplicados o incorrectos)
- **Fraude interno** por parte de empleados.
- **Ciberataques y robo de información** confidencial.
- **Fallas en los sistemas informáticos** que interrumpan las operaciones.

Actividades de Riesgo

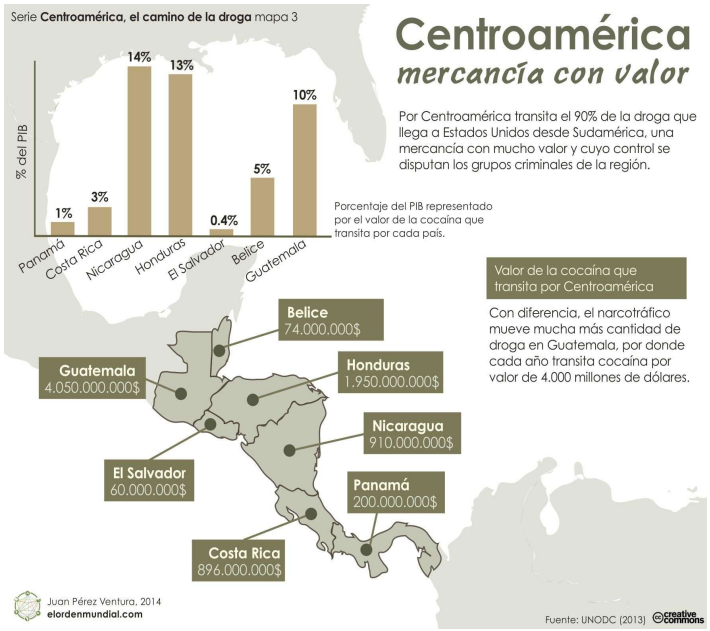
Riesgos de liquidez: No contar con suficiente en caja para cumplir con obligaciones diarias.

Riesgos Legal y de Cumplimiento: Este riesgo se deriva del incumplimiento de leyes, regulaciones o contratos. Ejemplo, normas contra el lavado de dinero (AML).

Riesgo Reputacional: Se refiere a perdidas por daño en la imagen y confianza de los ciudadanos.

- **Escándalos públicos por prácticas no éticas o negligencia.**
- **Filtración de información.**
- **Mal servicio prestado**.

Riesgo Estratégico: Riesgo por decisiones que pueden impactar negativamente la institución a largo plazo.



RUTA DEL DINERO

La ruta del dinero

Para identificar la ruta del dinero es fundamental rastrear el movimiento de los fondos y considerar las transacciones claves para lograr una trazabilidad detallada. Y así entender el origen, movimiento y destino de los fondos, lo cual es crucial para el cumplimiento normativo, detección de fraudes y análisis de riesgos.

La ruta del dinero

Ruta del dinero (origen)

- **Depósitos y transferencias**, identificar origen de los fondos.
- **Información detallada** del origen de los mismos.
- **Medios de Ingreso**, efectivo, transferencia, depósitos, etc.
- **Movimientos** internos, transacciones que permiten la materialización del dinero y sus etapas.
- **Transferencias** interbancarias, ACH (Automated Clearing House, Swift (Transferencias internacionales, LBTR(Sistema de liquidación Bruta en Tiempo Real), etc.
- **Instrumentos** financieros utilizados.

Ruta del dinero (Destino)

- **Retiros** en efectivo.
- **Pagos y transferencias** salientes, Detalle de destinatarios y entidades receptoras.
- **Inversiones y pagos** de servicios, fondos utilizados para adquirir productos, pago de prestamos y servicios públicos.

La ruta del dinero

Registros (Movimientos)

- **Temporalidad** (TimeStamps), Fecha y hora exacta de cada transacción.
- **Número de referencia único** de la operación para su rastreo.
- **Cantidad** exacta y tipo de moneda.
- **Institución y/o ubicación**, lugar físico exacto o virtual donde se realiza la operación.

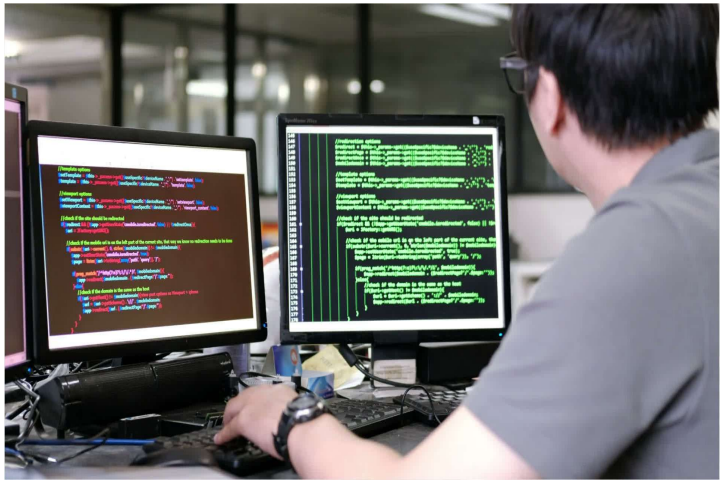
Ruta del dinero (Cuentas y productos)

- **Manejo de las cuentas** corrientes utilizadas. Con detalle de movimientos. Incluir en esta nuevas modalidades como **Criptomonedas**.
- **Tarjetas de Crédito o debito** utilizadas, seguimiento de compras, pagos y retiros.
- **Prestamos y líneas de crédito**, aplicación y uso de los fondos que se originan de adquisición de créditos o donaciones.

La ruta del dinero

Transacciones Clave para la Trazabilidad

1. Depósitos y retiros en efectivo.
2. Transferencias electrónicas (locales e internacionales).
3. Pagos con tarjeta (POS, comercio electrónico).
4. Transacciones de compra/venta de divisas.
5. Préstamos y pagos de créditos.
6. Inversiones en instrumentos financieros (acciones, bonos, fondos).
7. Donaciones.
8. Pagos de servicios o facturas recurrentes.
9. Transacciones sospechosas o no habituales.
10. Criptomonedas.



BITACORAS

Bitácoras (logs)

Las bitácoras(logs) En las entidades son registros críticos que documentan las actividades de los eventos de un sistema. La correcta gestión y construcción de las bitácoras garantizan la seguridad, el cumplimiento normativo y trazabilidad de los procesos.

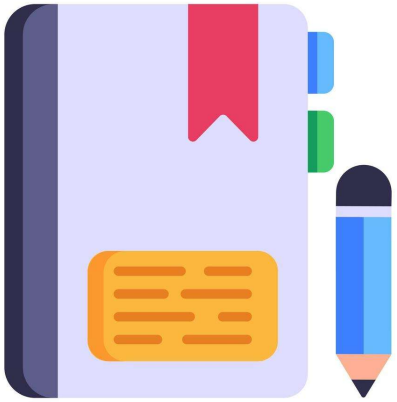
Definir una política de Bitácoras

- **Establecer estándares,** aquí se definen que eventos deben ser registrados, nivel de detalle y tiempo que se almacenará la información.
- **Cumplimiento normativo**, Que la política cumpla con regulaciones establecidas. (SOX, PCI, DSS, ISO 27001).

Registro de información Clave

- Determinar la información mínima por evento, Ejemplo: Fecha y hora exacta, Usuario, ID del proceso, Dirección IP y ubicación (considerar accesos remotos o conexiones), Descripción del evento(Acceso exitoso, fallo, modificación de datos, etc.) Resultado de la operación (Éxito, fallo, error, denegado, etc.), Sistema, nivel de criticidad.

Bitácoras (logs)



Eventos de la bitácora por categorías

- **Eventos de seguridad,** es importante contar con una descripción ejemplo “intento de acceso fallido”, cambios de permisos, autenticaciones fallidas.
- **Eventos operativos**, Errores del sistema, caídas de servicios, ejecuciones de procesos críticos.
- **Eventos de transacciones**, Operación de autorización de pago, transferencia de fondos, pagos, retiros.
- **Eventos administrativos**, Actualización de configuraciones, instalación de parches o cambios de infraestructuras.

Seguridad y protección de las bitácoras

- **Inmutabilidad**, Las bitácoras creadas deben ser protegidas contra modificaciones. Utilizando técnicas como el hashing y el equipos de almacenamiento en **WORM (Write Once, Read Many)**.
- **Control de acceso**, Solo personal autorizado debe tener acceso a las bitácoras, siguiendo el **principio de mínimos privilegios**.
- **Cifrado**, almacenar y transmitir las bitácoras de manera cifrada para proteger la información y asegurar la confidencialidad.

Bitácoras (logs)

Almacenamiento y retención

- **Almacenamiento Seguro,** contar con servidores dedicados para almacenar bitácoras y que se cuente con una solución de replicación en diferente ubicación y backup.
- **Política de retención de información**, definir en esta los periodos de retención claros, considerando la criticidad de los eventos. Ejemplo:
  - Eventos críticos, almacenar por 5 a 10 años.
  - Eventos operativos generales durante 1 a 2 años.
- **Archivado automático**, implementar procesos nocturnos que permitan mantener las bitácoras antiguas sin afectar el rendimiento.

Monitoreo y Análisis continuo

- **Implementar herramientas de monitoreo**, por ejemplo implementación de SIEM (Security Information and Event Management) para realizar el análisis automatizado de las bitácoras.
- **Alertas automáticas**, configurar alertas cuando suceden patrones sospechosos o anomalías, por ejemplo múltiples intentos fallidos de inicio de sesión de los equipos.
- **Análisis forense**, estas bitácoras facilitan el análisis detallado en caso de incidentes de seguridad.

Bitácoras (logs)

Integridad y Sincronización de Tiempos de Equipos de Hardware

- **Servidor NTP (Network Time Protocol),** Para garantizar que los registros sean correctos y que brinden información importante y trazabilidad, equipos donde se ejecutan los sistemas deben estar sincronizados con un servidor de tiempo confiable, para evitar inconsistencias.

Auditorias periódicas y pruebas

- **Revisiones regulares**, se debe tener un plan de auditoria periódico para garantizar que las bitácoras estén bien y cumplen con los estándares definidos en la política.
- **Pruebas de recuperación**, realizar pruebas para asegurar que las bitácoras puedan recuperarse en caso de incidentes o fallos.

Capacitación e información documentada

- **Manual de procedimientos**, contar con información documentada de como se generan, almacenan y se realiza la revisión de las bitácoras.
- **Capacitación**, realizar entrenamiento al personal en el uso y la interpretación de las bitácoras para facilitar el monitoreo y detección de problemas.

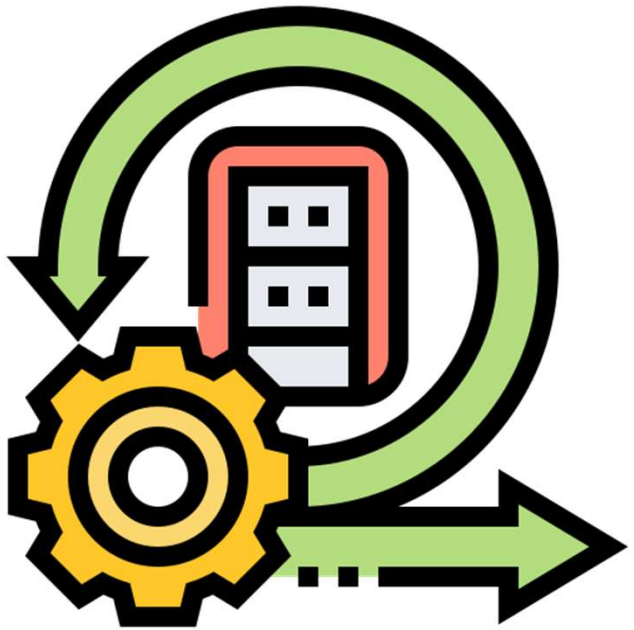
Mejores prácticas

Desarrollar software de manera segura, aplicando prácticas y procesos que ayuden a proteger las aplicaciones de ataques cibernéticos y vulnerabilidades.

1. Considerar **la seguridad desde el diseño** de la aplicación, realizando un análisis de riesgo y amenazas durante el diseño.
2. Realizar **pruebas de seguridad**, pruebas de caja negra, pruebas de caja blanca, pruebas de penetración (pentesting)
3. Utilizar **buenas prácticas de codificación** (OWASP Secure Coding Practices), manejar correctamente las validaciones y el ingreso de datos de entrada.
4. Mantener **la ultima versión de librerías** utilizadas por la herramienta de desarrollo. Como también de los otros componentes de software utilizado.

Mejores prácticas

5. Utilizar **controles de autenticación y autorización** robustos, aplicando MFA- Autenticación Multifactor. Dar accesos del menor privilegio, control de sesiones seguros y expiración de sesiones automáticamente.
6. **Revisiones** de código periódicas.
7. **Cifrado de datos** sensibles durante su transmisión y almacenamiento.
8. **Llamada a otras aplicaciones y API** de forma segura.
9. **Gestión segura de configuraciones**, no almacenar contraseñas en el código y desactivar lo que no se utilizará en ambiente de producción.
10. **Manejo de errores e implementación de bitácoras y monitoreo**, para detectar actividades sospechosas.
11. **Capacitación continua a desarrolladores** en tema de seguridad. Se recomienda talleres y ejercicios de simulación de ataques.



Características de Calidad

La **calidad del software** se puede determinar y evaluar considerando diferentes atributos, el estándar ISO/IEC 25010 define ocho características principales y sus subcategorías. Entre ellas tenemos:

Funcionalidad

- **Adecuación funcional**, si cumple con los requerimientos del usuario.
- **Exactitud**, los resultados proporcionados son correctos y se proporcionan con precisión.
- **Interoperabilidad**, la capacidad que tiene el software de interactuar con otros sistemas.

Características de Calidad

Eficiencia de desempeño

- **Tiempos de respuesta**, las solicitudes son atendidas en un tiempo adecuado.
- **Recursos utilizados**, los recursos de los servidores son utilizados de manera optima, CPU, Memoria, etc.
- **Capacidad**, manejo de grandes volúmenes de datos y accesos de usuarios sin demeritar su funcionamiento.

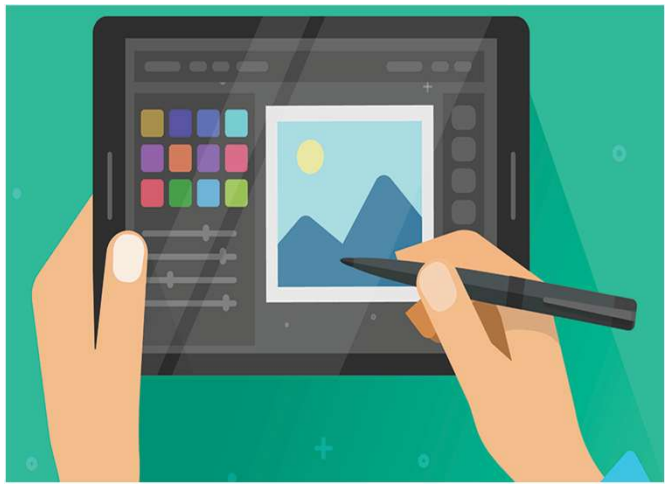
Compatibilidad

- **Coexistencia**, el funcionamiento es correcto al interactuar con otros sistemas.
- **Portabilidad**, se puede ejecutar en varios entornos, sin tener que realizar modificaciones.
- **Fácil de instalar** y configurar.
- **Adaptabilidad**, fácil de adaptarse a nuevos entornos.

Características de Calidad

Usabilidad

- **Intuitivo y Amigable**, es fácil de entender y utilizar para nuevos usuarios.
- **Aprendizaje**, cuenta con información de ayuda y mensajes que facilitan el aprendizaje.
- **Accesibilidad**, puede ser usado por personas con capacidades especiales.



Confiabilidad

- **Madurez del software**, esta libre de errores y fallos recurrentes.
- **Disponibilidad**, el sistema funciona en horarios cuando se necesita.
- **Tolerancia a fallos**, es la capacidad que tiene de recuperarse de errores.

Características de Calidad

Seguridad

- **Confidencialidad**, utiliza mecanismos de protección y enmascaramiento de los datos sensibles.
- **Integridad**, el sistema evita modificaciones no autorizadas.
- **Autenticidad**, utiliza métodos de verificación de identidades adecuadamente.
- **Trazabilidad**, cuenta con registros o bitácoras para auditar acciones realizadas en el sistema. Y realizar el diagnostico de problemas.

Mantenibilidad

- **Modularidad**, los cambios y mejoras se pueden realizar por partes.
- **Reusabilidad**, capacidad de reutilizar los componentes.
- **Capacidad de pruebas**, debido a su diseño facilita la forma de hacer pruebas.

Mejores Prácticas en Sistemas de Información

- **Automatización de proceso:** Construir sistemas que permitan registrar automáticamente información que alimenten al sistema de Calidad.

- **Digitalización:** Sustituir formularios en papel por formularios electrónicos y procesos automatizados de validación y autorización con mecanismos de firmas digitales avanzadas.

- **Trazabilidad Completa:** Hacer el registro de las *etapas del proceso y asegurar que los sistemas registren cualquier cambio* automáticamente para facilitar auditorias y detección de fallos.

Estándares de calidad

Existen varios estándares de calidad orientados al desarrollo de software que ayudan a garantizar que los sistemas sean seguros, eficientes y cumplan con lo solicitado por el usuario. Veamos los siguientes:

ISO (Organización Internacional de Normalización)

ISO 9001:2015

- Se enfoca en la **Gestión de la calidad**, cuyo objetivo es establecer los procesos que **garanticen** que los **productos y servicios** cumplan con los **requerimientos del cliente**. Esto se aplica los procesos de desarrollo del software.

ISO/IEC 25000 (Software Quality Requirements and Evaluation)

- Su enfoque es la **Calidad del producto de software** y establece los **criterios para evaluar la calidad** del mismo; características importantes: Funcionalidad, fiabilidad, usabilidad, eficiencia, mantenibilidad y portabilidad.