GESTIONANDO RIESGOS E IDENTIDADES DE NUESTRA PROFESIÓN

consejo
Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires

Objetivo

Orientar a los **profesionales de Ciencias Económicas y a la sociedad...**

- ...sobre las buenas prácticas relacionadas a accesos a sistemas y/o aplicativos con el objetivo principal de preservar la **integridad** y **confidencialidad** de la información.
- ...a una línea de ***pensamiento basada en riesgo*** que les permita *identificar* y *gestionar* de una manera dinámica los riesgos, independientemente del marco de desempeño.

Escenario inicial

Escenario inicial

SAP ERP
Microsoft Dynamics
PeopleSoft
THOMSON REUTERS DISTRIBUIDOR OFICIAL
TANGO gestión
ORACLE JD EDWARDS
ORACLE ERP CLOUD
INTERbanking

Procesos relevantes de Seguridad en Aplicativos

Control de Acceso

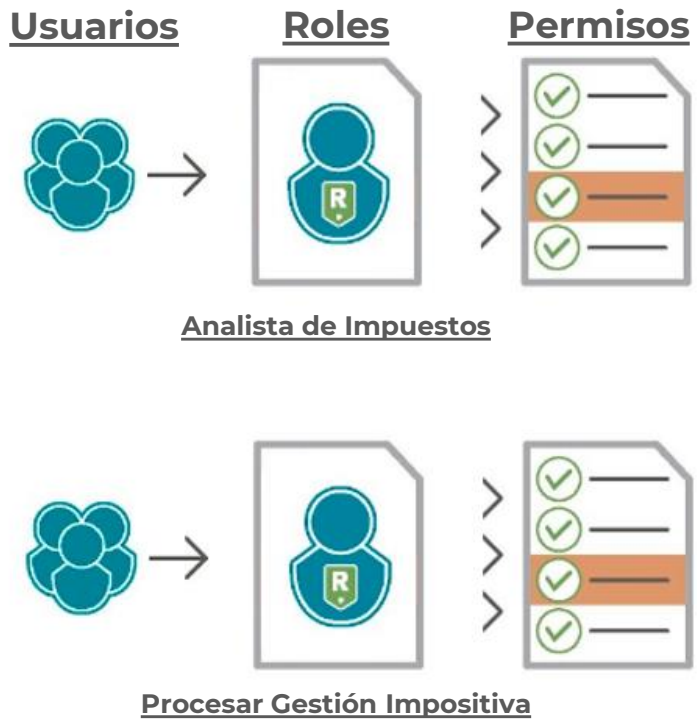
- Proceso que incluye la definición e implementación de medidas de seguridad para la protección de las **identidades** que utilizan un sistema o aplicativo que tiene como uno de sus objetivos garantizar que tengan **acceso** a **los datos y funciones** de acuerdo a **su puesto laboral.**

- Dentro del proceso se destaca:

  - ✓ Método de autenticación e inicio de sesión (usuario y contraseña).
  - ✓ Definición de Roles/Perfiles en base a puestos laborales.
  - ✓ Definición de accesos críticos.
  - ✓ Segregación de funciones.
  - ✓ Definición de responsables.

Roles de usuario

- El acceso basado en **roles** se refiere a los derechos de acceso que se pueden asignar a un usuario o un equipo en una organización de acuerdo a las funciones que realiza.
- Un rol es un **conjunto de "permisos"**. Cuando un usuario es asignado a un rol, se les otorga los acceso a visualizaciones y funciones definidas en él.
- La buenas prácticas establecen que un rol debe estar **siempre asociado a un perfil de puesto** o **a un proceso**.



Segregación de Funciones (SOD)

Es un método relacionado a la gestión de riesgos y controles internos de una organización que se basa en las **responsabilidades compartidas** de un proceso clave que **dispersa las funciones críticas** en más de una persona. Dentro de las ventajas de tener una correcta SOD se encuentran: **reducción de ocurrencias de errores**, **mitigación de ocurrencia de fraudes**, **generación de un ambiente de control**, entre otros.

En caso de ausencia de no contar con suficiente personal para separar las tareas en más de una persona, se puede considerar la implementación de controles.

SOD - Algunos ejemplos

- Tareas que deben estar separadas en **cualquier proceso**.

1. Generación de un comprobante.
2. Autorización del comprobante.

- Tareas que deben estar separadas de un proceso de **compras**.

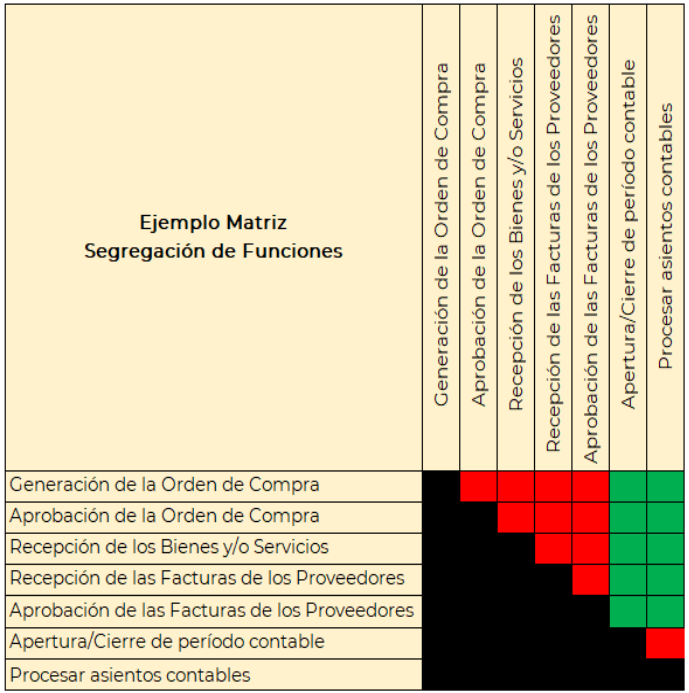
1. Generación de la Orden de Compra.
2. Aprobación de la Orden de Compra.
3. Recepción de los Bienes y/o Servicios.
4. Recepción de las Facturas de los Proveedores.
5. Aprobación de las Facturas de los Proveedores.

- Algunas tareas que deben estar separadas de un proceso de **RRHH**.

1. Alta de empleados/as.
2. Liquidación de Salarios.
3. Autorización y/o Ejecución del Pago.

- Tareas que deben estar separadas en un proceso **contable**.

1. Apertura/Cierre de período contable.
2. Procesar asientos contables.



SOD - Algunos ejemplos

LA NACION

LA NACION > Economía

Al menos 10 empleados de Aerolíneas estafaban a la empresa pagándose sobresueldos

25 de octubre de 2018 • 16:57

Jerónimo Mura y Julia D'Arrisso

La empresa Aerolíneas Argentinas fue sacudida por una estafa por parte de un grupo de empleados que cobraban "gastos excepcionales" en la liquidación se sus salarios por encima de lo que les correspondía.

Según pudo reconstruir **LA NACION**, un total de 10 empleados de Aerolíneas liquidaban costos adicionales sobre el total del salario a otros empleados y luego se repartían la diferencia por transferencia bancaria. Un grupo de ellos pertenecía al área de Liquidaciones, mientras que el resto estaba distribuido en otros rubros.

El sistema comenzaba al momento de pagar los sueldos, donde se cargaban valores adicionales en concepto de "gastos excepcionales". Luego, el beneficiario recaudaba y repartía el dinero extra entre los involucrados. Una vez realizado el pago, se borraba el detalle de los saldos del sistema con el que la empresa lleva su contabilidad.

SOD - Algunos ejemplos

IPROFESIONAL

IPROFESIONAL | LEGALES | EN LA PLATA

Phishing: condenaron al Banco Provincia a pagar $600.000 a un cliente que sufrió una estafa

La jueza María Cecilia Tanco, titular del Juzgado Civil y Comercial N° 19 de La Plata, condenó al Banco Provincia al pago de una multa de 600.000 pesos por un caso de phishing contra el jubilado y cliente de la entidad Daniel Ricardo Suarez.

Además, la magistrada condenó a la entidad bancaria a la devolución del monto de adelanto de haberes de 22.500 pesos que fuera tomado por un grupo de personas que utilizaron la técnica de "phishing" para estafar a un jubilado de 68 años pidiendo un crédito de 650.000 pesos en su nombre y cobrando un adelanto de su jubilación. También se declaró la nulidad de este último.

"Se pudo determinar que surgían del log de transacciones operaciones en las que se involucraban montos importantes que no recibieron el tratamiento que correspondía por su carácter de sospechosas o potencialmente fraudulentas", especificó la jueza.

Además, Tanco manifestó que tampoco se cumplió "con el control de acceso, **el cual es un proceso relacionado con la evaluación, desarrollo e implementación de medidas de seguridad** para la protección de la identidad, mecanismos de autenticación, segregación de roles y funciones, y demás características del acceso de los usuarios internos y externos a los canales electrónicos".

Responsabilidades – Matriz RACI

La **Matriz RACI** es una herramienta que permite representar la asignación de responsabilidades en un proyecto.
Describe el uso de varias funciones relacionadas con las actividades realizadas en una empresa.
Su nombre proviene de las funciones que permite reflejar.

- **R**esponsible (Responsable) -> Realiza el trabajo para completar una tarea.
- **A**ccountable (Aprobador) -> Se responsabiliza que la tarea se realice y es el que debe rendir cuentas sobre su ejecución.
- **C**onsulted (Consultor) -> Brindan opiniones de valor y puede tener información requerida para el proceso. (generalmente son expertos en el tema).
- **I**nformed (Informado) -> Informado sobre el avance y los resultados de la ejecución de la tarea.

Ejemplo de aplicación en el proceso de compra de una computadora.

Tares\Responsable	Sector Solicitante	Analista de Compras	Gerente de Compras	Analista Cuentas a Pagar	Gerente de Administración	Sistemas
Generación de la Orden de Compra	I	R	A			C
Aprobación de la Orden de Compra	I	I	R			
Recepción de los Bienes y/o Servicios	R	I	I	I		
Recepción de las Facturas de los Proveedores		I	I	R	A	
Aprobación de las Facturas de los Proveedores			I	I	R	

¿Por qué es importante el rol de los Matriculados?

Los Profesionales de Ciencias Económicas tienen un papel decisivo para colaborar en la implementación de controles de accesos en los Sistemas y Aplicativos ya que pueden:

- Asesorar y colaborar en la definición de **accesos críticos**.
- Sugerir **casos de tareas** que deben estar **separadas por presentar un riesgo.**
- Colaborar en la definición de **controles (manuales/automáticos)** en aquellos casos donde la separación de tareas en distintas personas no es posible de aplicar.
- Asesorar y colaborar en la confección de **procedimientos y matrices** en base a su conocimiento de los procesos implementados en los sistemas y/o aplicativos.

Conclusiones finales y buenas prácticas

- Evitar el uso de super usuarios y con accesos amplios.
- Tener en los sistemas o aplicativos solos los accesos necesarios para realizar las funciones.
- Considerar solicitar permisos temporales para funciones esporádicas que no son rutinarias.
- No compartir credenciales de accesos con colegas.
- Considerar una segregación de funciones en procesos claves que permitan la eliminación de errores involuntarios o fraudes.
- Definir responsabilidades para dar claridad en procesos y funciones claves.

Antecedentes

- **Factor Humano como eslabón más débil**
- Credenciales de acceso
- B.E.C
- Phishing
- Ransomware
- Wifi
- IoT
- Infraestructura
- Disrupción
- Super usuarios
- Segregación de funciones

Factor Común

INFORMACIÓN

Ejemplo de Clasificación de Riesgos

- Relacionados a los RRHH
- Falla o mal funcionamiento de un proceso y/o sistema tecnológico
- Cultura de la Organización, etc

Riesgos Operativos

Riesgos Financieros

- Mercados
- Crédito
- Liquidez, etc

Riesgos del Negocio/Alta Dirección

Riesgos Accidentales

- Políticos
- Económicos
- Sociales
- Tecnológicos
- Conocimientos, etc

- Inmuebles
- Personas
- Responsabilidades Legales, etc

Tipos de Controles

Tipos de Control	Interviene en la ponderación del Impacto	Interviene en la ponderación de la Probabilidad
Mitiga o reduce el riesgo	X	
Prevé el riesgo		X

- **Controles Estructurales:** Son implementados al momento del desarrollo y actúan por si solos.
- **Controles Pasivos:** Pueden ser implementados en el desarrollo o posteriormente y una vez ejecutados requieren intervención para volver a su estado original.
- **Controles Activos:** Son implementados a demanda y requieren la intervención de personal capacitado para la tarea.

Ejemplo Tipos de Impacto y variables

Tipos de Impacto
Pérdida económica
Incumplimiento legal y/o regulatorio
Daño reputacional
Afectación del servicio al cliente
Pérdida de capacidad productiva
Daño a la salud y/o bienestar de las personas

VARIABLES	
PROBABILIDAD	IMPACTO
Muy Improbable	Muy bajo
Improbable	Bajo
Eventualmente	Medio
Probable	Alto
Poco Probable	Muy Alto

FORTALEZA DE LOS CONTROLES	
Clasificación	Efecto
Sin Control	No modifica ninguna de las variables
Necesita Mejoras	Reduce al menos una de las variables en un nivel
Aceptable	Reduce al menos una de las variables en dos niveles
Satisfactorio	Reduce al minimo alguna de las variables
Muy Satisfactorio	Reduce al minimo ambas variables

Fórmulas:

Nivel de Riesgo = Probabilidad x Impacto

Nivel de Riesgo = Probabilidad x Impacto x Causas

Inherente

CONTROLES

Residual

Inherente: que no se puede separar de él por formar parte de su naturaleza y no depender de algo externo

Residual: Es el remanente que queda posterior a la aplicación de controles

Riesgos de Cumplimiento

PRODUCTOS PROCESOS	REGULACION	REQUERIMIENTO	CONSECUENCIA
Liquidación Impuesto a las Ganancias	Ley 20.628 (to.1997) y modificatorias R.G. (AFIP) 992	Cumplir con la presentación de la DDJJ anual, el pago del impuesto determinado y de los anticipos	Sanciones: Ley 11.683 Ley 24.769
Liquidación Impuesto a la Ganancia Mínima Presunta	Ley 25.063 y modificatorias	Cumplir con la presentación de la DDJJ anual, el pago del impuesto determinado y de los anticipos	Sanciones: Ley 11.683 Ley 24.769
Liquidación Impuesto al Valor Agregado (IVA)	Ley 23.349 y modificatorias	Cumplir con la presentación de las DDJJ mensuales y el pago del impuesto determinado	Sanciones: Ley 11.683 Ley 24.769
Liquidación de retenciones y percepciones de IVA y Ganancias	R.G.(AFIP)18 R.G.(DGI) 3337 R.G.(AFIP) 830 R.G.(AFIP) 738	Cumplir con la presentación de las DDJJ mensuales y el pago quincenal de las retenciones y percepciones efectuadas	Sanciones: Ley 11.683 Ley 24.769

PRODUCTOS PROCESOS	REGULACION	REQUERIMIENTO	CONSECUENCIA
Pagos a Beneficiarios del Exterior	Ley 20.628 (to.1997) y modificatorias Ley 23.349 y modificatorias	Análisis de la retención de ganancias a efectuar al beneficiario del exterior. Pago de IVA por importación de servicios	Sanciones: Ley 11.683 Ley 24.769
Liquidación de Ingresos Brutos	Codigos Fiscales de cada provincia. RG (CA) 72	Cumplir con la presentación de las DDJJ mensuales y el pago del impuesto. Presentar DDJJ anual	Sanciones: Codigos Fiscales de cada provincia.
Liquidación de retenciones y percepciones de Ingresos Brutos de la Ciudad Autónoma de Buenos Aires	R (SHyF) 430 R (DGR CBA) 1359	Cumplir con la presentación de las DDJJ mensuales y el pago de las retenciones y percepciones efectuadas	Sanciones: Código Fiscal
Liquidación de retenciones y percepciones de Ingresos Brutos de la Provincia de Buenos Aires	DN (DPR) "B" 1/2002	Cumplir con la presentación de las DDJJ mensuales y el pago de las retenciones y percepciones efectuadas	Sanciones: Código Fiscal

PRODUCTOS PROCESOS	REGULACION	REQUERIMIENTO	CONSECUENCIA
Régimen de información: Retenciones y percepciones (SIRCAR)	R.G. (CA) 77 Codigos fiscales de las provincias adheridas	Presentación mensual por internet de percepciones y retenciones sufridas de ingresos brutos	Sanciones: Codigos Fiscales de cada provincia.
Emisión de Facturas	Normas internas (Circulares y Pedidos de Facturación)	Cumplimiento de las normas internas en cuanto a cantidades y precios facturados	Facturación incorrecta Reclamo de clientes
Emisión de Facturas	R.G. (AFIP) 1415	Cumplimiento del régimen de emisión de comprobantes	Sanciones: Ley 11.683
Registración de Facturas de Proveedores	Normas internas (Requisiciones, niveles de autorización)	Cumplimiento de las normas internas en cuanto a cantidades y precios facturados	Registración incorrecta Reclamo de proveedores
Registración de operaciones	R.G. (AFIP) 1361	Cumplimiento del régimen de registración de operaciones	Sanciones: Ley 11.683
Régimen de información: Cruzamiento informático de transacciones importantes (CITI)	R.G. (AFIP) 781	Presentación de la declaración jurada mensual	Sanciones: Ley 11.683

PRODUCTOS PROCESOS	REGULACION	REQUERIMIENTO	CONSECUENCIA
Pago a proveedores: Medios de pago	Ley 25.345 R.G. (AFIP) 1547 Ley de cheques 24.452	Autorización de pagos. Utilizar los medios de pago permitidos. Firma conjunta de dos apoderados.	Pagos erróneos. Imposibilidad del cómputo de deducciones y créditos fiscales
Cobranzas de clientes	Normas internas	Cobranzas efectuadas a clientes segun clausulas contractuales y a bancos por compensacion	Errores en las cobranzas. Reclamos de clientes
Régimen de información: Control de pago de autónomos	R.G. (AFIP) 167	Presentación trimestral de nota indica	Sanciones: Ley 11.683
Administración de Contratos	Normas internas	Cumplimiento de requisitos formales y legales. Requerir el cumplimiento de las clausulas contractuales	Penalidades especificadas en las clausulas del contrato
Contratación de seguros	Normas internas	Asegurar los bienes de la compañía debido a posibles contingencias	Pèrdida de activos

PRODUCTOS PROCESOS	REGULACION	REQUERIMIENTO	CONSECUENCIA
Archivo de comprobantes y documentación de respaldos y libros contables	Ley 11.683	Conservación de la documentación de las operaciones por el término de 10 años	Ley 11.683
Documentación Comercial	Código de Comercio - Artículo 44 y 67 -	Conservar la documentación comercial por el plazo de 10 años	Código de Comercio
Régimen de información: Informe para fines fiscales	R.G. (AFIP) 992	Presentación de la declaración jurada anual con información sobre libros rubricados	Sanciones: Ley 11.683
Presentación de Estados Contables en la IGJ	Ley 19.550	Presentación de los Estados Contables anuales y Convocatoria a Asamblea.	Sanciones: Ley 19.550
Régimen de información: Participaciones societarias	R.G. (DGI) 4120	Presentación de la declaración jurada anual	Sanciones: Ley 11.683
Régimen de información: Donaciones	R.G. (AFIP) 1675	Presentación de la declaración jurada anual	Sanciones: Ley 11.683

Responsabilidad

- *Civil*
- *Penal*
- *Profesional*

Preguntas de guía

- ¿Hasta dónde estoy dispuesto a aceptar los daños de un riesgo?
- ¿El riesgo de mi proceso u operación incluye algún riesgo de otro tipo?
- ¿El nivel de riesgo es inherente o residual?
- ¿La criticidad de mi proceso impacta a procesos transversales y/o superiores?
- ¿Mi análisis de riesgo contemplo toda la cadena de procesos?
- ¿Qué escenarios de riesgos considere?
- ¿Utilice algún marco metodológico?
- ¿Quiénes participaron de la evaluación?
- ¿Las variables utilizadas en mi análisis, poseen sustento y objetividad?
- ¿Cada cuánto tiempo hago la revisión de mi análisis? ¿Cuándo fue la última revisión?

Conclusión

- **Es primordial establecer los parámetros que voy a utilizar.** *(Marco normativo o metodológico, herramientas, variables, tipos de control, etc)*

- **No hay gestión de riesgos mejor que otra, el nivel de éxito está asociado directamente al resultado.** *(Un análisis de riesgos efectivo puede medirse de forma concreta al final de cada ciclo analizando las amenazas contenidas contra las ejecutadas)*

- **Es importante mantener actualizada mi gestión de riesgos y el chequeo de los controles.** *(La gestión de los riesgos y evaluación de controles debe estar en constante movimiento, atento a los cambios y necesidades del contexto)*

Links para profundizar

El 75% de los gestores de riesgos desconoce si el impacto de las criptomonedas en la economía será cuantificable

Escrito por ANTONIO NOGUERAS | Categorías CIBERSEGURIDAD Y RIESGOS DIGITALES | Fecha 1 AGOSTO, 2022 | Comentarios 0 COMENTARIOS

El 64% de los gestores de riesgos consideran que las criptomonedas tendrán un impacto relevante sobre el sistema financiero global. Sin embargo, de ellos, el 75% reconoce no saber ni cuánto ni cuándo será ese impacto. Así lo revela la **EALDE Risk Survey 2022**, una encuesta realizada por **EALDE Business School** en la que han participado más de 1.000 profesionales de habla hispana interesados en la gestión del riesgo y la incertidumbre.

"Las criptomonedas suponen un cambio de paradigma desde un sistema fiduciario tradicional, controlado por los bancos centrales y los gobiernos, a unas finanzas descentralizadas, que pretenden crear un sistema financiero más transparente y fuera del control de las empresas y los gobiernos", indica Enrique Farrás, director de **EALDE Business School**.

De esta forma, las criptomonedas permiten reducir costes y burocracia en las transacciones de activos y facilitan el acceso a capital por vías no centralizadas. No obstante, la alta volatilidad que tienen las criptomonedas también suponen un reto para los gestores de riesgos. "Muchos ahorradores van a pedir a las sociedades de inversión que parte de sus ahorros se inviertan en criptomonedas. Sin embargo, **estas inversiones siguen siendo de alto riesgos, dada la volatilidad del valor de los criptoactivos**", añade el experto.

Riesgos de lavado de activos

Otro desafío que presenta la tecnología cripto son los riesgos de estafa y blanqueo de capitales que pueden surgir a raíz del uso de las criptomonedas en el mercado global. De hecho, ya en 2019, el Grupo de Acción Financiera Internacional (GAFI) emitió una guía en la que destacaba que los activos virtuales generan oportunidades para que "lavadores de dinero, financiadores del terrorismo y otros criminales laven sus ganancias o financien sus actividades ilícitas".

En este sentido, en España **el Ministerio de Hacienda ya prepara una Ley Antifraude que, a partir de enero de 2023**, obligará a los titulares de criptomonedas a declarar las operaciones y saldos que tengan de estos activos.

EALDE Business School es una escuela especializada en ofrecer formación online para la identificación, caracterización y mitigación de riesgos financieros, crediticios, legales o reputacionales, como los que pueden derivarse del uso de criptomonedas.

Si quieres obtener más información acerca del Máster en Riesgos Digitales, Ciberseguridad y Continuidad de Negocio, puedes hacer clic en el siguiente botón:

https://www.ealde.es/impacto-de-las-criptomonedas-en-la-economia-global/ (Link de la nota)

https://www.ealde.es/blog-ealde/

https://www.youtube.com/c/EaldeEs

¿Preguntas?

¡Muchas Gracias!