TEMA 08.
DIAGNÓSTICO DE RIESGOS. MAPA DE RIESGOS Y CONTROLES.

ALBERT SALVADOR

LICENCIADO EN CC ECONÓMICAS Y EMPRESARIALES. AUDITOR INTERNO CERTIFICADO POR EL IIA (THE INSTITUTE OF INTERNAL AUDITORS). ESPECIALISTA EN FRAUDE INTERNO, FORENSIC Y PREVENCIÓN DE BLANQUEO DE CAPITALES. SECRETARIO GENERAL Y MIEMBRO DE LA JUNTA DIRECTIVA DE LA WORLD COMPLIANCE ASSOCIATION.

LAURA GONZALVO DILOY

COMPLIANCE OFFICER ACREDITADA POR WCA. LICENCIADA EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS. MÁSTER EN AUDITORÍA Y EN GESTIÓN Y DIRECCIÓN DE ENTIDADES NO LUCRATIVAS. CHIEF COMPLIANCE OFFICER DE LA FUNDACIÓN AYUDA EN ACCIÓN. MIEMBRO DEL GRUPO DE TRANSPARENCIA Y ANÁLISIS NORMATIVO DE LA CONGDE.

EXPLICACIÓN DEL CONCEPTO

Un mapa de riesgos es una herramienta basada en los distintos sistemas de información que pretende identificar las actividades o procesos sujetos a riesgo, cuantificar la probabilidad de estos eventos y medir el daño potencial asociado a su ocurrencia. Un mapa de esta naturaleza proporciona tres valiosas contribuciones a un gestor: proporciona información integrada sobre la exposición global de la empresa, sintetiza el valor económico total de los riesgos asumidos en cada momento, y facilita la exploración de esas fuentes de riesgo.

El mapa se instrumenta en un panel gráfico interactivo, a modo de cuadro de mando, que enfatiza las anomalías o desviaciones y permite que el usuario navegue a lo largo de los indicadores en diferentes niveles de desagregación.

El objetivo del mapa de riesgos es sintetizar la información relativa a las indeterminaciones que afronta la empresa y colaborar en las estrategias destinadas a mitigar la exposición y los daños potenciales. Empleamos la noción de indeterminación para referirnos a las circunstancias que condicionan el valor o el resultado de una transacción u operación, y que no están completamente bajo el control de la organización. Este planteamiento se corresponde con la noción clásica de riesgo: una indeterminación que puede ser medida en términos de probabilidad (Knight, 1921) y que implica una pérdida potencial con impacto financiero relevante.

CONSEJOS SOBRE CÓMO HACERLO

Los pasos establecidos para la elaboración de un mapa de riesgos se pueden clasificar en:

01. **Definición del contexto.**
02. **Identificación de los riesgos.**
03. **Análisis, asignación y valoración de los riesgos.**
04. **Identificación de controles.**
05. **Análisis, asignación y valoración de controles.**
06. **Establecimiento de opciones de tratamiento de los riesgos.**
07. **Monitoreo de los riesgos.**
08. **Revisión sistemática del mapa de riesgos.**

A continuación, se definen cada una de estas fases:

DEFINICIÓN DEL CONTEXTO

La administración del riesgo tiene como propósito principal detectar toda situación que pueda poner en riesgo el cumplimiento de los objetivos estratégicos de la organización o proyecto realizado, razón por la cual debe estar alineado con las directrices establecidas por el órgano de gobierno y el órgano de gestión.

IDENTIFICACIÓN DE RIESGOS

La identificación de riesgos posibilita conocer los eventos potenciales que pueden afectar el logro de los objetivos estratégicos de la organización y, por lo tanto, el cumplimiento de su misión. Igualmente, en esta fase se busca establecer los agentes generadores del riesgo, así como las causas y los efectos de su ocurrencia.

Para llevar a cabo la identificación del riesgo se deben utilizar metodologías de recolección de información y determinación de los riesgos existentes y potenciales de la organización. Algunos elementos de apoyo utilizados para la identificación de riesgos y amenazas son entrevistas con expertos en el proceso o área de interés; revisión de registros; lluvias de ideas y cuestionarios.

La identificación de riesgos debe realizarse con una periodicidad mínima anual, para así actualizar la taxonomía de riesgos y poder confirmar aquellos que siguen siendo significativos, eliminar aquellos que ya no apliquen e incorporar los nuevos emergentes, puesto que el contexto en el que opera la organización y sus necesidades son dinámicos.

Si lo que vamos a desarrollar es un mapa de riesgos para los riesgos penales, debemos tener en cuenta aquellas actividades de la organización que puedan desencadenar uno de los delitos tipificados en el Código penal español (Ley Orgánica 10/1995, de 23 de noviembre):

1. Tráfico y trasplante ilegal de órganos (art. 156.3 bis).
2. Trata de seres humanos (art. 177 bis 7).
3. Delitos relativos a la prostitución y a la explotación sexual y corrupción de menores (art. 189 bis).
4. Descubrimiento y revelación de secretos y allanamiento informático (art. 197 quinquies).
5. Estafa (art. 251 bis).
6. Frustración en la ejecución (art. 258 ter).
7. Insolvencias punibles (art. 261 bis).

8. Daños informáticos (art. 264 quáter).
9. Delitos contra la propiedad intelectual e industrial, al mercado y a los consumidores (y corrupción en los negocios) (art. 288).
10. Blanqueo de capitales (art. 302.2).
11. Financiación ilegal de partidos políticos (art. 304 bis 5).
12. Delitos contra la Hacienda pública y la Seguridad Social (art. 310 bis).
13. Delitos contra los derechos de los ciudadanos extranjeros (art. 318 bis).
14. Delitos contra la ordenación del territorio y el urbanismo (art. 319).
15. Delitos contra los recursos naturales y el medio ambiente (art. 328).
16. Delitos relativos a la energía nuclear y radiaciones ionizantes (art. 343.3).
17. Delitos de riesgo provocados por explosivos y otros agentes (art. 348.3).
18. Delitos contra la salud pública (art. 366).
19. Delitos contra la salud pública (tráfico de drogas) (art. 369 bis).
20. Falsificación de moneda (art. 386.5).
21. Falsificación de tarjetas de crédito y débito y cheques de viaje (art. 399 bis).
22. Cohecho (art. 427 bis).
23. Tráfico de influencias (art. 430).
24. Delitos de incitación del odio, hostilidad, discriminación o violencia (art. 510 bis).
25. Financiación del terrorismo (art. 576).
26. Contrabando (art. 2, LO de represión del contrabando).
27. Relativos a la manipulación genética (art. 162).
28. Alteración de precios en concursos y subastas públicas (art. 262).
29. Negativa a actuaciones inspectoras (art. 294).
30. Delitos contra los derechos de los trabajadores (art. 318).
31. Asociación ilícita (art. 520).
32. Organización y grupos criminales y organizaciones y grupos terroristas (art. 570 quáter).

VALORACIÓN DE RIESGOS

Una vez categorizado el riesgo, se deberá asignar a uno o a varios procesos de la organización, en los cuales tendremos identificados los departamentos que intervienen. En organizaciones que no dispongan de procesos identificados y procedimentados, será necesario elaborar un mapa de los procesos más significativos de la organización, identificando a un responsable de los mismos.

Para la valoración de los riesgos, nos apoyaremos en una matriz de riesgos de doble entrada:

- Probabilidad/Frecuencia
- Impacto/Severidad.

Las matrices más utilizadas son las de 3x3 y las de 5x5, siendo estas últimas las que se usan con más frecuencia y que detallaré más adelante.

Evaluar la probabilidad e impacto de los potenciales riesgos es un proceso en el que hay que contar con factores monetarios o económicos, financieros, operacionales, reputacionales y legales. No todos los riesgos potenciales tienen la misma probabilidad y el mismo impacto en todos los casos.

PROBABILIDAD

Se entiende por ésta la probabilidad de que el riesgo se concrete en un suceso cierto, antes de considerar cualquier control o acción mitigadora. La evaluación de la probabilidad de ocurrencia de un determinado riesgo considera factores como la ocurrencia en la organización de ese riesgo en el pasado, su frecuencia en las organizaciones del mismo sector, la complejidad del riesgo y el número de personas involucradas en la revisión y aprobación del proceso, entre otros factores. Evaluada la probabilidad de ocurrencia, ésta se categoriza en función de la matriz utilizada. En una matriz de 5x5 tendríamos los siguientes tramos, los cuales pueden ser adaptados a las necesidades de la organización: rara; improbable, posible, probable y casi segura.

IMPACTO

Se entiende por impacto al daño que supondría para los objetivos estratégicos de la organización que el riesgo se concretara en un suceso cierto. La evaluación del impacto de que un riesgo finalmente se materialice, no solo tiene en cuenta factores monetarios en los estados financieros, sino también factores operacionales, reducción del rendimiento de la actividad, el valor de la marca, pérdida de imagen, la reputación, aspectos legales y regulatorios. Al igual que con la probabilidad de ocurrencia, una vez evaluado el impacto de que un riesgo de fraude se materialice, éste se categoriza.

PROBABILIDAD							
	5	CASI CIERTO	MEDIO	ALTO	ALTO	CRÍTICO	CRÍTICO
	4	PROBABLE	BAJO	MEDIO	ALTO	ALTO	CRÍTICO
	3	POSIBLE	BAJO	MEDIO	MEDIO	ALTO	ALTO
	2	IMPROBABLE	MUY BAJO	BAJO	MEDIO	MEDIO	ALTO
	1	RARO	MUY BAJO	MUY BAJO	BAJO	BAJO	MEDIO
			INSIGNIFICANTE	MENOR	MODERADO	MAYOR	SEVERO
			1	2	3	4	5
			IMPACTO				

(GRÁF.1)

En una matriz de 5x5 tendríamos los siguientes tramos, los cuales pueden ser adaptados a las necesidades de la organización: insignificante, menor, moderado, mayor impacto, severo.

Finalizado este proceso obtenemos el Riesgo Inherente, que, en función de la probabilidad e impacto, y usando la matriz de riesgos (graf. 1), lo clasificaremos en: Muy Bajo, Bajo, Medio, Alto, Crítico.

IDENTIFICACIÓN DE CONTROLES

De manera análoga a la fase identificación de riesgos, mediante el conocimiento y análisis de la organización, preferiblemente a través de sus procesos documentados, se procede a la identificación de los controles. Estos controles permitirán en última instancia o bien reducir la probabilidad de ocurrencia de un suceso o, si éste se produce, minimizar su impacto.

VALORACIÓN DE CONTROLES

Una vez identificados los controles, volveremos a calcular el riesgo al que está sometida la organización, pero esta vez considerando el nivel de vulnerabilidad actual de los controles disponibles en la organización. Para el cálculo de este riesgo consideramos la siguiente fórmula (teniendo en cuenta, esta vez sí, la variable de vulnerabilidad): **RIESGO RESIDUAL = P X I X V**

Para poder calcular la efectividad de los controles, nos podemos basar en diferentes ítems de valoración, con sus diferentes criterios, como por ejemplo: Tipo de Control: Preventivo, Detectivo o Correctivo; Frecuencia en su ejecución y seguimiento; Ocasional, Periódico o Permanente; Metodología de Realización: Manual, Semiautomático o Automático.

El grado de efectividad del control determinará el grado de reducción que proporciona ese control sobre un determinado riesgo. Estas metodologías de cálculo deben estar previamente definidas y procedimentadas.

ESTABLECIMIENTO DE OPCIONES DE TRATAMIENTO DE LOS RIESGOS

Una vez calculado el riesgo residual se podrán priorizar los riesgos que forman parte de nuestra taxonomía inicial, los cuales podrán ser clasificados y adaptados a las necesidades de cada organización según decisión del órgano de gobierno u órgano de gestión.

En base a esta categorización, la organización deberá seleccionar aquellos riesgos sobre los que enfocar el correspondiente monitoreo. Una vez estos hayan sido seleccionados, se deberá asignar un propietario del riesgo, siendo éste el responsable del proceso con el que está mayoritariamente relacionado.

Partiendo de la base de que todos los riesgos o situaciones de riesgos son objeto de seguimiento y de acciones correctivas o mitigadoras, es el órgano de gobierno o el órgano de gestión quien define los criterios de tratamiento de los riesgos, es decir, el nivel de riesgos sobre los cuáles va a priorizar su gestión, centrando su atención y recursos.

Las opciones para el tratamiento de los riesgos evaluados pueden consistir en reducir el riesgo (reducir amenazas, vulnerabilidades, posibles impactos, etc.) implantando las medidas o salvaguardas apropiadas; transferir el riesgo a terceros, por ejemplo, suscribiendo una póliza de seguros o un contrato con proveedores o socios; aceptar el riesgo, lo que implica no hacer nada porque no se puede, dado el carácter del riesgo, o porque éste se encuentra dentro de los niveles aceptables; evitar el riesgo, esto es, no proceder con la actividad que genera el riesgo.

El tratamiento de riesgos se desarrolla a través de un plan de acción de riesgos, estableciendo las medidas que se implantarán en el caso de aquellos riesgos identificados como no aceptables, y que, por tanto, superen el «apetito de riesgo» que haya establecido el órgano de gobierno o el órgano de gestión.

El Informe COSO, documento que contiene las principales directivas para la implantación, gestión y control de un sistema de control, define el apetito de riesgo como como el nivel aceptable de variación en los resultados o actuaciones de la organización relativas a la consecución o logro de sus objetivos estratégicos. Dicho de otra manera, el riesgo que se está dispuesto a aceptar en la búsqueda de la misión/visión de la entidad.

MONITOREO DE LOS RIESGOS

El monitoreo de los riesgos es una parte clave de cualquier plan de gestión de riesgos de cualquier organización, ya que permite determinar si todos los componentes del plan de prevención operan efectivamente y si el resultado de los controles identificados es reportado oportunamente al órgano de *compliance*.

Para el monitoreo de los riesgos se definirán indicadores cuantitativos o cualitativos, así como los controles asignados; lo que constituye el plan de acción. En caso de que un indicador supere la tolerancia fijada, serán los propietarios de los riesgos los encargados de analizar las causas.

El órgano de *compliance* deberá monitorizar la correcta aplicación de los planes mencionados. Así, la efectiva labor de monitoreo no sólo contribuye a realizar análisis de causa, sino que permite identificar qué procesos son vulnerables a estos riesgos y con base a ello desarrollar nuevos planes de acción.

REVISIÓN SISTEMÁTICA DEL MAPA DE RIESGOS

Como se verá en el capítulo 19 en profundidad, se deben revisar los riesgos vigentes y deben estar actualizados de acuerdo con los nuevos riesgos identificados. Para garantizar que el sistema de gestión de riesgos sea sólido y eficaz, esta revisión se debe realizar al menos una vez al año por parte de los responsables de procesos, o con mayor frecuencia en caso de cambios organizacionales significativos, cambios importantes en tecnología, en los objetivos estratégicos de negocios, en el entorno de la organización, etc. Con independencia de las revisiones generales planificadas, es un mundo ideal, los riesgos deberían estar permanente actualizados.

EJEMPLOS PRÁCTICOS

Ejemplo de diagnóstico en 6 pasos:

1. **Identificación de riesgos**
2. **Valoración de riesgos**
3. **Identificación de controles**
4. **Valoración de controles**
5. **Umbral de riesgo**
6. **Plan de acción**

Nos vamos a centrar en el delito de descubrimiento y revelación de secretos y allanamiento informático (art. 197 *quinquies*).

Tendríamos las siguientes conductas delictivas:

04.01. Apoderarse de papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales para descubrir los secretos o vulnerar la intimidad de otro sin su consentimiento.

04.02. Interceptar las telecomunicaciones o utilizar artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra

señal de comunicación, para descubrir los secretos o vulnerar la intimidad de otro sin su consentimiento.

04.03. Sin estar autorizado, apoderarse, utilizar o modificar, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado, o acceder por cualquier medio a esa misma información y alterarla o utilizarla en perjuicio del titular de los datos o de un tercero.

04.04. Difundir, revelar o ceder a terceros datos o hechos descubiertos o imágenes captadas, incluso si no se ha tomado parte en su descubrimiento pero conociendo su origen ilícito

04.05. Acceder o facilitar a otro el acceso a un sistema de información, vulnerando las medidas de seguridad establecidas y sin estar autorizado

04.06. Utilizar artificios o medios técnicos, sin estar autorizado, para interceptar transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información

04.07. Producir, adquirir, importar o facilitar a terceros un programa informático concebido o adaptado para cometer delitos relacionados con el descubrimiento y revelación de secretos.

04.08. Producir, adquirir, importar o facilitar a terceros una contraseña de ordenador o código de acceso que permitan el acceso total o parcial a un sistema de información

Estas serían las actividades de riesgo pueden desencadenar alguna de estas conductas delictivas:

Recogida de cartas, paquetes, notificaciones, etc.

Recogida y tratamiento de datos de carácter personal de empleados, proveedores, clientes o terceros con quien la organización tenga una relación empresarial y/o contractual.

Grabación por parte de las cámaras de seguridad.

Uso de dispositivos móviles de cualquier tipo (teléfonos, tabletas electrónicas, USB etc.) sin el debido control

Revisión, monitorización y acceso al correo electrónico y equipos informáticos de los empleados por parte de la organización.

PASO 1 – IDENTIFICACIÓN DE RIESGOS

La parte de la identificación de riesgos es el pilar básico del mapa de riesgos, ya que todo el sistema de gestión de riesgos parte de los riesgos identificados.

Por ello, es muy importante identificar aquellas acciones que se puedan comentar en el seno de las organizaciones y que puedan desencadenar la responsabilidad penal de la empresa. Luego, hemos de ir detectando cuáles son aquellas actividades que se realizan o pueden realizar en el seno de nuestra organización que desencadenen estas conductas de riesgo.

Por lo tanto, una manera eficaz de identificación de riesgos sería hacer un recorrido por todos los procesos de la organización y verificar que actividades se pueden dar del catálogo de conductas. Este recorrido lo haremos mediante entrevistas con los diferentes responsables, cuestionarios y el conocimiento de la organización y la legislación del *Compliance Officer.*

Para este ejemplo vamos a partir de la siguiente actividad de riesgo:

«Recogida de cartas, paquetes, notificaciones, etc. Recogida y tratamiento de datos de carácter personal de empleados, proveedores, clientes o terceros con quien la organización tenga una relación empresarial o contractual. Uso de dispositivos móviles de cualquier tipo (teléfonos, tabletas electrónicas, USB etc.) sin el debido control. Revisión, monitorización y acceso al correo electrónico y equipos informáticos de los empleados por parte de la organización.»

IMPORTANTE:

Una vez identifica la conducta de riesgo, vamos a asignarla a un proceso (o departamento en caso de no disponer de un mapa de procesos):

Tipo de Riesgo	Descripción del Riesgo	Conducta de Riesgo	Proceso
04. Delitos contra la intimidad y el allanamiento informático	04.01. Apoderarse de papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales para descubrir los secretos o vulnerar la intimidad de otro sin su consentimiento	Recogida de cartas, paquetes, notificaciones, etc. Recogida y tratamiento de datos de carácter personal de empleados, proveedores, clientes o terceros con quien la organización tenga una relación empresarial y/o contractual. Uso de dispositivos móviles de cualquier tipo (teléfonos, tabletas electrónicas, USB, etc.) sin el debido control. Revisión, monitorización y acceso al correo electrónico y equipos informáticos de los empleados por parte de la organización.	Gestión de Administración

PASO 2 – VALORACIÓN DE RIESGOS

A continuación, procederemos a la valoración del riesgo, asignando una Probabilidad y un Impacto:

El resultado de la Probabilidad x Impacto será el RIESGO INHERENTE.

En este caso hemos asignado una Probabilidad de Probable (4) y un Impacto de Moderado (3), por lo que el Riesgo inherente es: 4 x 3 = 12

Probabilidad	Impacto	Riesgo Inherente
Probable (4)	Moderado (3)	Riesgo Alto (12)

Si aplicamos la tabla de valoraciones:

20 a 25	**CRÍTICO**	Necesidad de actuar con urgencia, el riesgo es inminente
10 a 19	**ALTO**	Actuar con celeridad probabilidad elevada de riesgo
5 a 9	**MEDIO**	Poco probable a corto plazo pero probable a medio/largo plazo
3 a 4	**BAJO**	Posibilidad baja de riesgo, asumible por la organización
1 a 2	**MUY BAJO**	Posibilidad de riesgo prácticamente nula

Tenemos que 12 equivale a **RIESGO ALTO.**

PASO 3 – IDENTIFICACIÓN DE CONTROLES

El siguiente paso corresponde a la identificación de controles, para lo que es importante un conocimiento de la organización, bien median la propia experiencia, las entrevistas con el personal implicado o cuestionarios.

Una vez identificados el control le asignamos un Departamento y persona responsable, y comprobamos que efectivamente se está realizando.

Controles existente	Departamento responsable del control	Responsable del Control	Realización
Cumplimiento con la normativa de la LOPD	RR.HH	Albert Salvador	SI
Adecuación al Reglamento de la LOPD	RR.HH	Albert Salvador	SI

PASO 4 – VALORACIÓN DE CONTROLES

Se proponen 3 ítems para la valoración de controles: el tipo de control, la frecuencia y la realización. Aplicando la metodología adoptada para la gestión de riesgos, obtendremos la vulnerabilidad del control. En el caso de existir más de un control, las vulnerabilidades van multiplicando sobre la anterior.

Tipo de Control	Frecuencia	Realización	Evaluación Efectividad del Control	Vulnerabilidad	Riesgo Residual
Preventivo (3)	Permanente (3)	Manual (1)	ALTA	0,4	Riesgo BAJO
Preventivo (3)	Ocasional (1)	Manual (1)	BAJA	0,8	

- Partíamos de un Riesgo Inherente de Riesgo alto: Probabilidad (4) x Impacto (3) = 12.
- Aplicando la vulneración del primer control, tenemos que el Riesgo Inherente es de: 12 x 0,4 = 4,8.
- Si aplicamos la vulneración de segundo control, tenemos que: 4,8 x 0,8 =3,84.

Si aplicamos nuevamente la tabla de valoraciones.

20 a 25	**CRÍTICO**	Necesidad de actuar con urgencia, el riesgo es inminente
10 a 19	**ALTO**	Actuar con celeridad probabilidad elevada de riesgo
5 a 9	**MEDIO**	Poco probable a corto plazo pero probable a medio/largo plazo
3 a 4	**BAJO**	Posibilidad baja de riesgo, asumible por la organización
1 a 2	**MUY BAJO**	Posibilidad de riesgo prácticamente nula

Tenemos que 3,84 equivale a **RIESGO BAJO.**

PASO 5 – UMBRAL DE RIESGO

Para cada riesgo la organización establecerá un Umbral de Riesgo, es decir cuál es su tolerancia al riesgo.

Imaginemos que para este riesgo la organización ha definido un Umbral de Riesgo de Riesgo Bajo:

Riesgo Residual	Objetivo	¿Cumple el objetivo?
Riesgo BAJO	Riesgo MUY BAJO	X

Para este riesgo tendríamos que la organización no cumple con los objetivos de riesgo.

PASO 6 – PLAN DE MITIGACIÓN

También denominado Plan de Acción. En aquellos casos en que no se cumplan con los objetivos de riesgo, la organización deberá adoptar medidas adicionales de control. Estos planes de acción, deberán tener un responsable asignado y una fecha máxima de implementación.

Acción	Responsable	Fecha de Implementación
Establecimiento de un registro de entrada de cartas, paquetes, notificaciones, etc. Diseño de un protocolo en el que se designe el responsable de la recogida y entrega de los documentos y paquetes.	Albert Salvador	31 de marzo de 2019
Formación de la normativa de protección de datos de carácter personal, en particular, en lo que respecta a la recogida, tratamiento y cesión de datos. Difusión de los correspondientes documentos de seguridad en función del nivel de protección de los datos.	Albert Salvador	31 de marzo de 2019
Política de Seguridad de la Información: adopción y difusión del documento que recoja la delimitación del uso de la información y sistemas por parte de los empleados de forma ética y de forma exclusiva en el ámbito profesional. Control correo electrónico corporativo (este se reduce exclusivamente a un ámbito laboral)	Albert Salvador	31 de marzo de 2019
Implantación de un sistema de Seguridad Informático	Albert Salvador	31 de marzo de 2019
Realizar inventario de hardware y software	Albert Salvador	31 de marzo de 2019

El mapa de riesgos es la suma del diagnóstico de todas las conductas de riesgo identificadas, y es algo «vivo» dentro de las organizaciones:

(siguiente página) ->

MATRIZ DE LOS RIESGOS

	IDENTIFICACIÓN DE RIESGOS					VALORACIÓN RIESGOS		RIESGO INHERENTE	IDENTIFICACIÓN CONTROLES					VALORACIÓN CONTROLES					RIESGO RESIDUAL	UMBRAL DE RIESGO		PLAN DE ACCIÓN			
Ref.	Tipo de Riesgo	Descripción Riesgo	Conducta Riesgo	Proceso	Área Responsable	Probabilidad	Impacto	Riesgo inherente	Ref. Control	Controles existentes	Dpto. Responsable del control	Responsable del control	Realización	Tipo	Frecuencia	Realización	Evaluación efectividad del control	Vulnerabilidad	Riesgo residual	Objetivo	¿Cumple el Objetivo?	Acción	Responsable	Fechade implementación	Situación
04.02	04. Delitos contra la intimidad y el allanamiento informático	04.02. Interceptar las telecomunicaciones o utilizar artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, para descubrir los secretos o vulnerar la intimidad de otro sin su consentimiento.	Grabación con teléfonos móviles, cámaras o similar de reuniones, conversaciones telefónicas etc.	Control de los dispositivos de medición y seg.	Dirección Gerencia	Posible (3)	Moderado (3)	Riesgo MEDIO	-	-	-	-	-	-	-	-	-	-	Riesgo MEDIO	Riesgo MUY BAJO	X	Formación de empleados en materia de prevención de riesgos penales, específicamente en relación con este delito y dirigida a todas las personas de la organización ya que por sus especiales características puede ser cometido por cualquier empleado. Suscripción del Código de Conducta por parte de todos los empleados.	Asesoría Externa: XXXXXXXXXX Compliance Officer	 31/01/2019	REALIZADO NO REALIZADO
04.05	04. Delitos contra la intimidad y el allanamiento informático	04.05. Acceder o facilitar a otro el acceso a un sistema de información, vulnerando las medidas de seguridad establecidas y sin estar autorizado	Acceso a sistemas y equipos informáticos sin consentimiento.	Atención al Cliente	Dirección Gerencia	Posible (3)	Mayor (4)	Riesgo ALTO	C1.04.05	Medidas de seguridad de la información implantadas por los proveedores de software de la organización	Dirección Gerencia	Director Gerente	SI	Preventivo (3)	Permanente (3)	Automático (2)	MUY ALTA	0,2	Riesgo BAJO	Riesgo BAJO	✓	Elaboración de una política sobre seguridad de la información. Formación específica para los empleados en materia de prevención de riesgos penales con especial referencia a los delitos informáticos. Suscripción del Código de conducta por empleados y colaboradores de la organización	DIRECTOR GENERAL Asesoría Externa: XXXXXXXXXX Compliance Officer	31/12/2019 31/12/2019 31/01/2019	FASE DE IMPLEMENTACIÓN FASE DE IMPLEMENTACIÓN NO REALIZADO
05.05	05. Estafa	05.05 Atribuirse falsamente sobre una cosa mueble o inmueble facultad de disposición de la que carece, bien por no haberla tenido nunca, bien por haberla ya ejercitado, para enajenarla, gravarla o arrendarela a otro, en perjuicio de éste o de tercero.	Actos de disposición patrimonial de todo tipo sobre bienes sobre bienes de los que no se dispone de la titularidad	Auditoria Interna	Dirección Gerencia Área Administración	Improbable (2)	Mayor (4)	Riesgo MEDIO	C1.05.05 C2.05.05 C3.05.05	Auditoria interna Auditoria externa por tercero independiente Cumplimiento de políticas contables y fiscales de ABANCA	Área Administración Área Administración Área Administración	Director Financiero Director Financiero Director Financiero	SI SI SI	Detectivo (2) Detectivo (2) Preventivo (3)	Permanente (3) Periódico (2) Periódico (2)	Manual (1) Manual (1) Automático (2)	MEDIA BAJA ALTA	0,6 0,8 0,4	Riesgo MUY BAJO	Riesgo MUY BAJO	✓	Suscripción del Código ético por parte de empleados y colaboradores de la organización Formación en materia de protección prevención de delitos, e particular, delitos económicos.	Compliance Officer Asesoría Externa: XXXXXXXXXX	31/01/2019 31/12/2019	NO REALIZADO FASE DE IMPLEMENTACIÓN
06.01	06. Frustración de la ejecución	06.01. Alzar los bienes propios en perjuicio de sus acreedores	Alzamiento de bienes ante un futuro embargo	Auditoria Interna	Dirección Gerencia Área Administración	Improbable (2)	Mayor (4)	Riesgo MEDIO	C1.06.01 C2.06.01	Auditoria interna Auditoria externa por tercero independiente	Área Administración Área Administración	Director Financiero Director Financiero	 SI	Detectivo (2) Detectivo (2)	Permanente (3) Periódico (2)	Manual (1) Manual (1)	MEDIA BAJA	0,6 0,8	Riesgo BAJO	Riesgo MUY BAJO	X	Suscripción del Código ético por parte de empleados y colaboradores de la organización Formación en materia de protección prevención de delitos, e particular, delitos económicos.	Compliance Officer Asesoría Externa: XXXXXXXXXX	31/01/2019 31/12/2019	NO REALIZADO REALIZADO