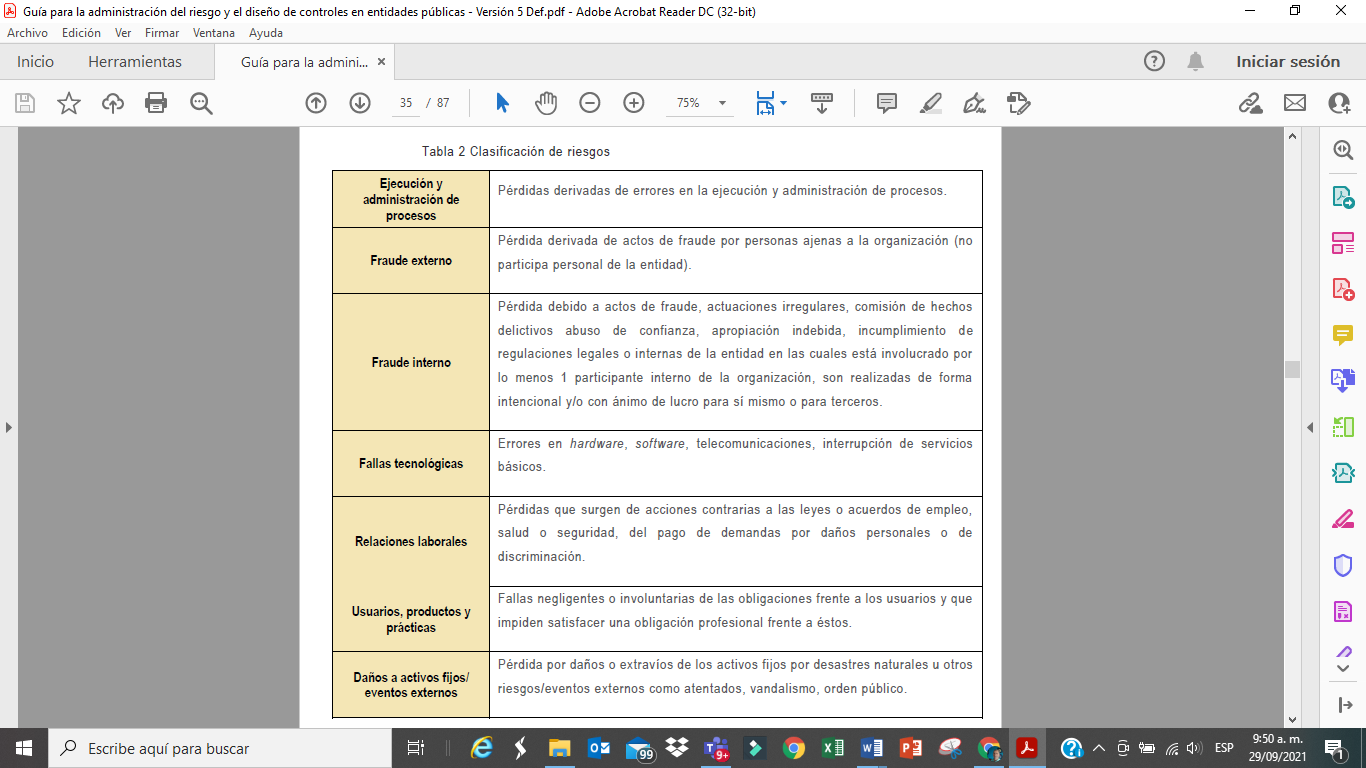
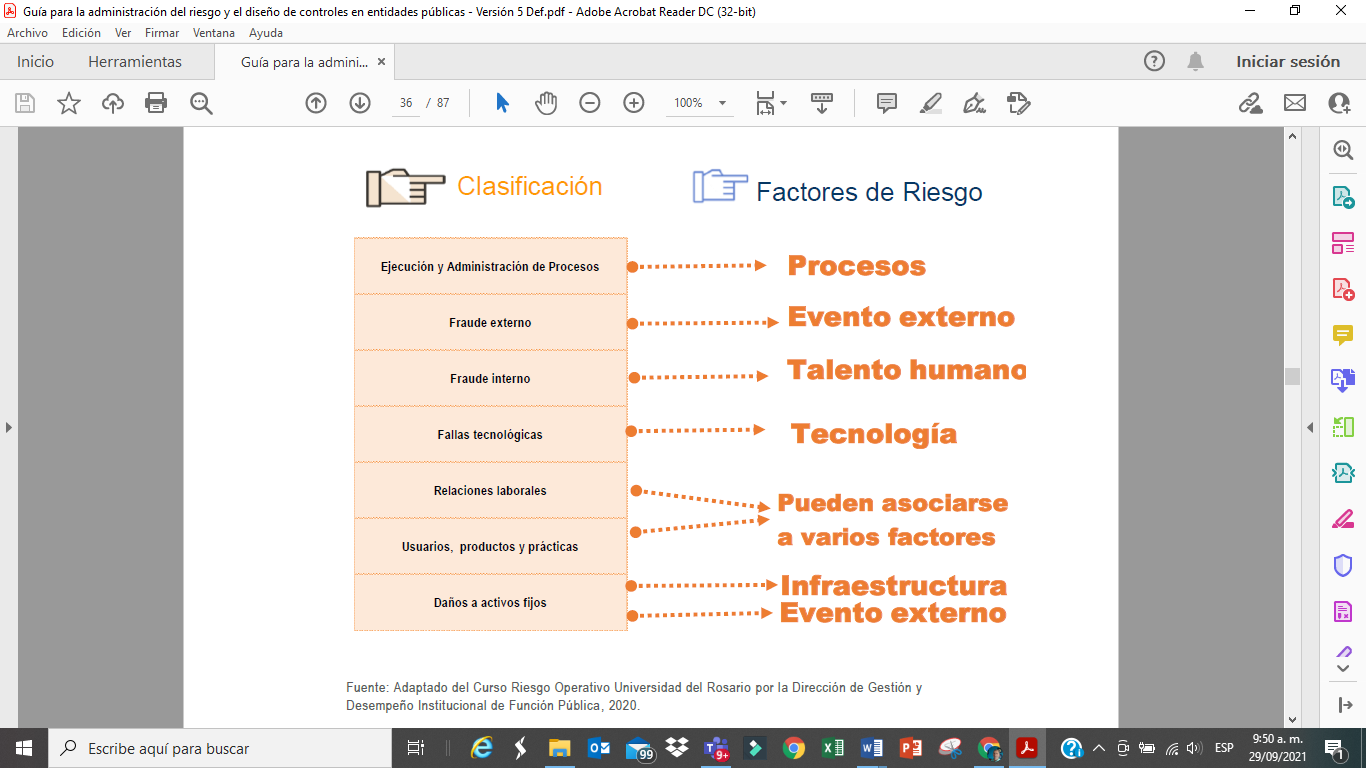
1. **IDENTIFICACIÓN DE RIESGOS**

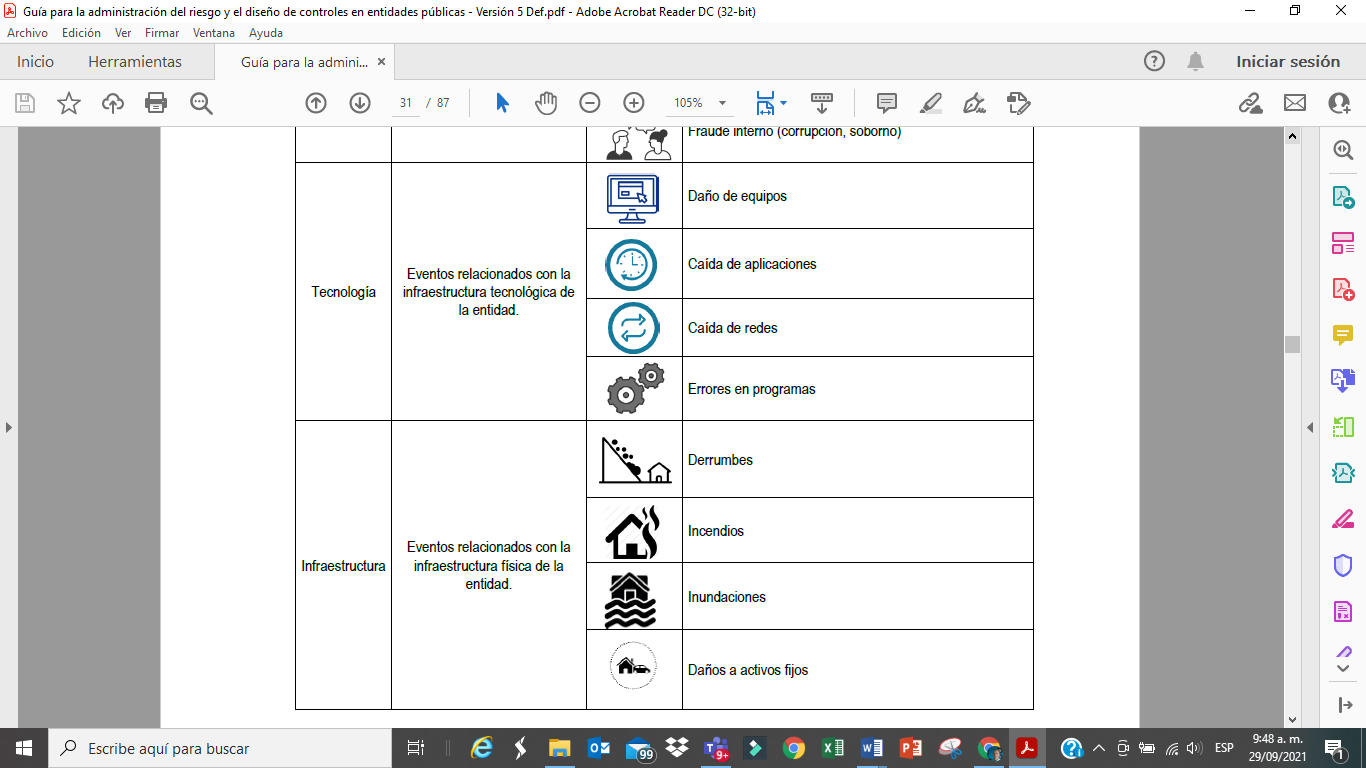
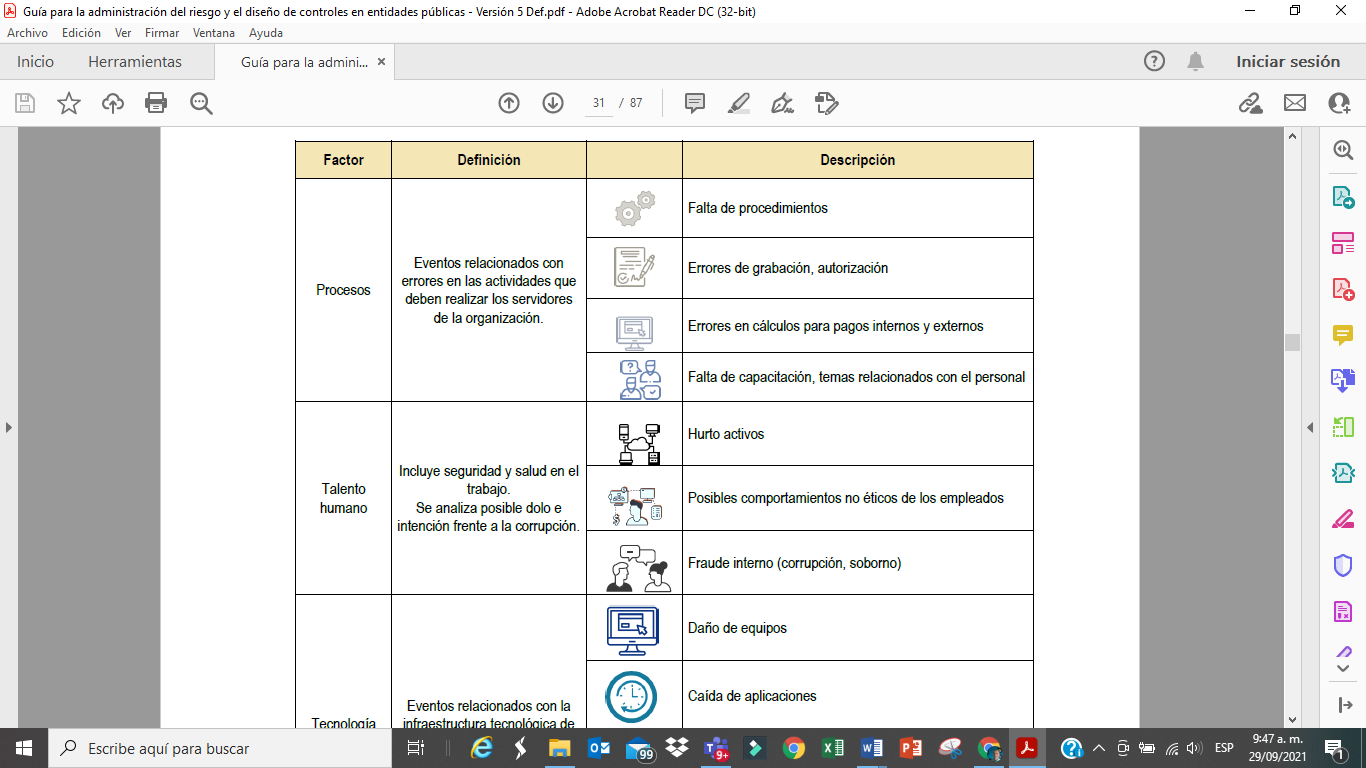
**Tabla No. 1. Clasificación de riesgos**

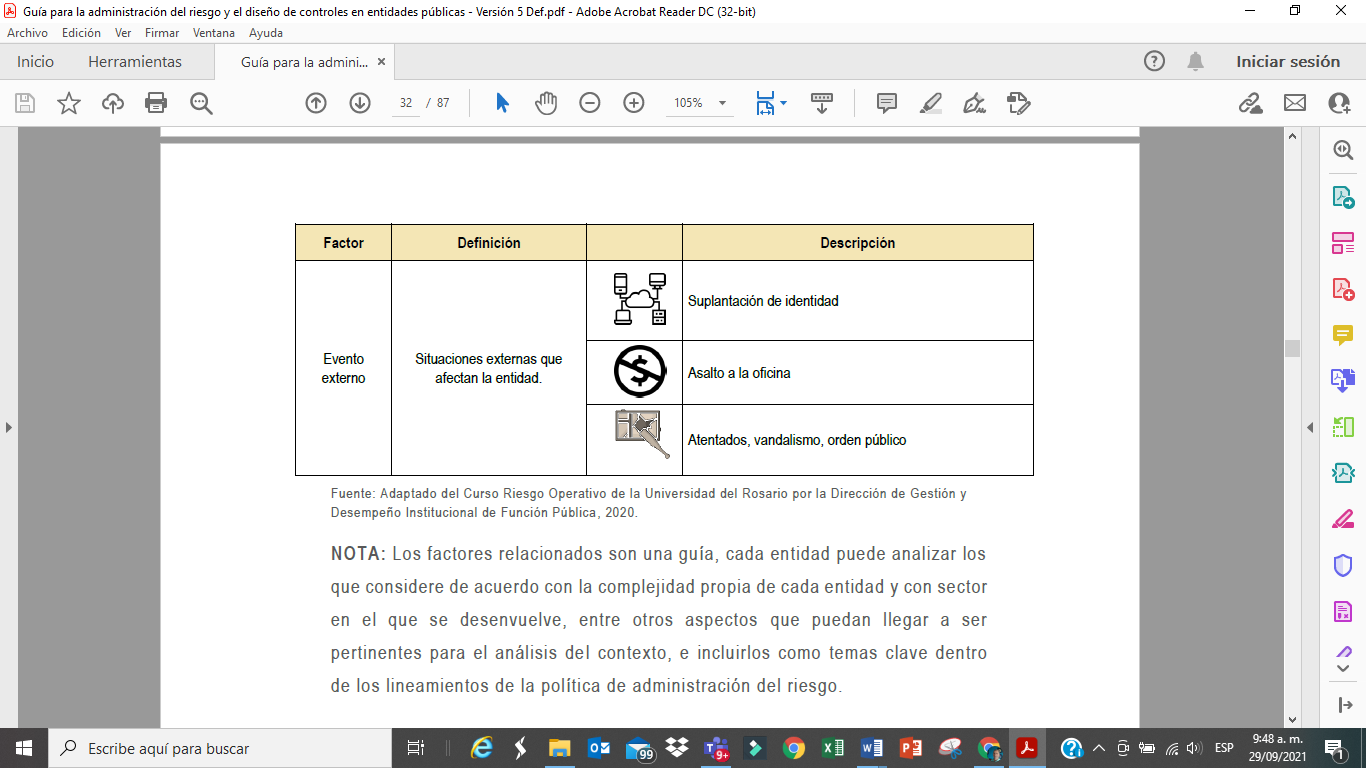


**Tabla No. 2. Clasificación del riesgo Vs factores de riesgos**



**Tabla No. 3. Factores de riesgos**





**Tabla No. 4. Puntos de Riesgo Fiscal**

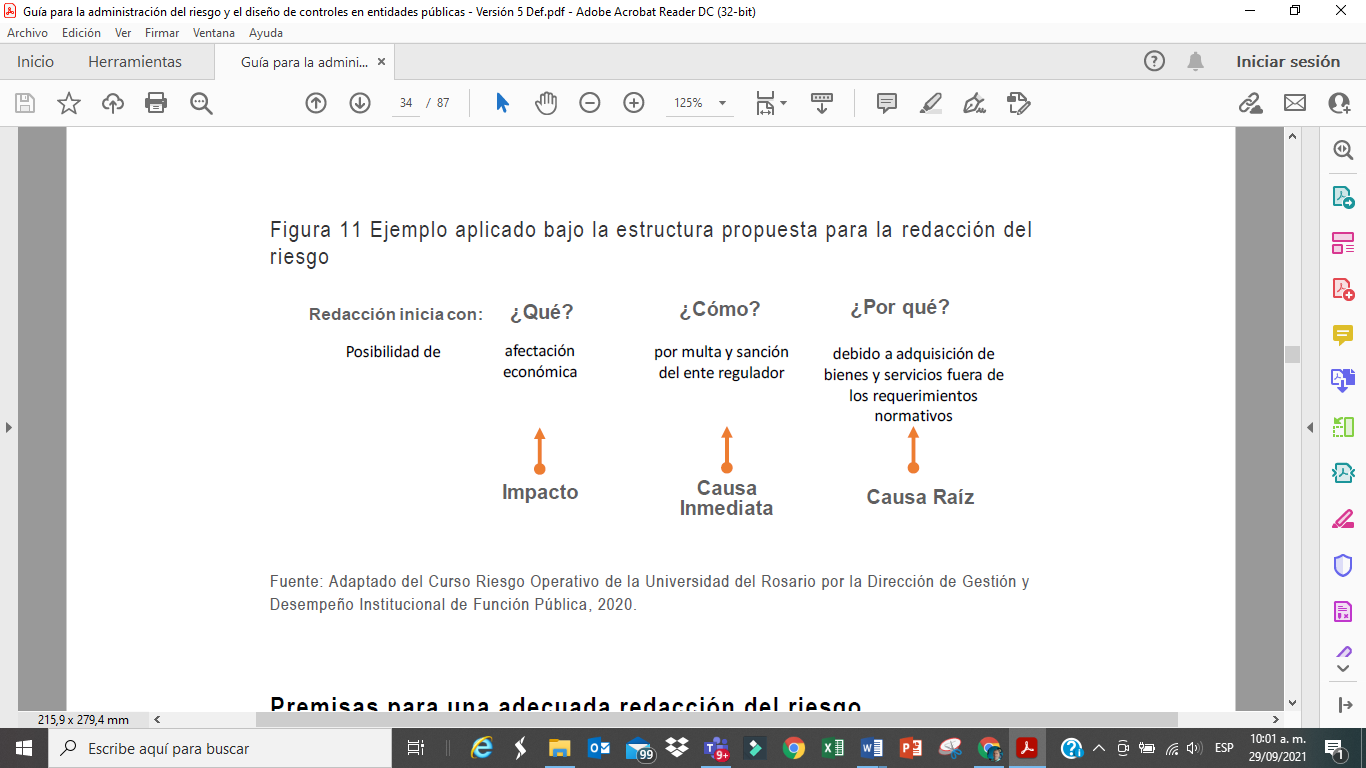
|  |
| --- |
| Los *Puntos de Riesgo Fiscal* corresponde a situaciones que hacen parte de la cotidianidad de la gestión pública, en las que se administran, gestionan, ordenan, ejecutan y/o recursos, bienes o intereses públicos y que potencialmente generan un efecto dañoso.  En este sentido y a partir del análisis de los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos cinco (5) años, se identificaron los siguientes Puntos de Riesgo, junto con las posibles circunstancias inmediatas, las cuales son enunciativas y no restrictivas: |

| **Puntos de Riesgo Fiscal** | **Circunstancia Inmediata** |
| --- | --- |
| **Actividad administrativa, contable y financiera** | * Pago de multas, cláusulas penales o cualquier tipo de sanción. * Pago de Intereses moratorios. * Pago de viáticos y gastos de desplazamiento sin justificación o por encima de los valores establecidos normativamente. * Mayor valor pagado por concepto de impuestos * Saldos o recursos a favor no cobrados. * Pérdida, extravío, hurto, robo o declaratoria de bienes faltantes pertenecientes a la Entidad. * Error en los avalúos, afectando el valor de venta y/o negociación de un bien público. * Incertidumbre en valores registrados en contabilidad. * Pagar bienes, servicios u obras a pesar de no cumplir las condiciones de calidad. * Mal manejo o fallas en la legalización de anticipos, no amortización del anticipo. * Rendimientos financieros de recursos de anticipo o de cualquier recurso público no devueltos al tesoro público * Reconocimiento y pago de desequilibrio contractual por causa imputable a la Entidad * Inadecuada deducción de impuestos, tasas o contribuciones al contratista * Vencimiento de plazos para la labor de cobro directo (persuasivo o coactivo) o judicial. * Daño en bienes muebles de propiedad de la entidad. * Pérdida de la tenencia de bienes inmuebles de la Entidad. |
| **Actividad de Defensa Judicial** | * Falencias en la defensa judicial que dan lugar a fallos condenatorios en contra de la Entidad. * Intereses moratorios por pago tardío de sentencias y conciliaciones. * Caducidad de la acción de repetición o falencias en el ejercicio de esta acción, generando la imposibilidad de recuperar los recursos pagados por el Estado. * Conciliación por baja probabilidad de éxito, debido a acciones u omisiones de la Entidad. * Vencimiento de términos en los procesos judiciales. * Debilidades en el inventario de procesos judiciales. * Conciliación por baja probabilidad de éxito, debido a acciones u omisiones de la Entidad. * Caducidad de la acción de repetición o falencias en el ejercicio de esta acción, generando la imposibilidad de recuperar los recursos pagados por el Estado. * Omisión en la obligación de impulsar acción judicial para cobrar clausula penal u otros perjuicios. |
| **Actividad de la Etapa Precontractual** | * Contratación de bienes y servicios no relacionados con las funciones de la Entidad. * Compra o inversión en bienes innecesarios o suntuosos. * Estudios y diseños recibidos y pagados y que no cumplen condiciones de calidad. * Estudios y diseños sin amparo de calidad del servicio. * Estudios y diseños con amparo de calidad vencido al momento de contratar la obra y/o al momento de la ocurrencia. * Insuficiencia de estudios previos. * Falencias o ausencia de estudio del mercado y/o análisis del sector, que genera sobrecostos o pagos que no representan beneficio público. * Matriz de riesgos insuficiente respecto a la realidad del contrato y/o proyecto. * Matriz de riesgos descontextualizada respecto a la realidad del contrato y/o proyecto. * Insuficiencia de las garantías exigidas. * Acuerdos restrictivos de la competencia, cotizaciones artificialmente altas u otras prácticas que alteran la realidad del mercado, generando sobrecostos. |
| **Actividad de la Etapa Contractual** | * Bienes, servicios u obras pagados, sin haber sido recibidos a satisfacción. * Recibo a satisfacción y consecuente pago de bienes, servicios u obras pagados, sin cumplir las condiciones contractuales y/o condiciones de cantidad y/o calidad. * Bienes, servicios u obras inconclusos, no funcionales y/o que no brindan utilidad o beneficio. * Modificaciones contractuales imputables al contratista total o parcialmente y cuyos costos colaterales asume la Entidad contratante. * Mal manejo o fallas en la legalización de anticipos, no amortización del anticipo. * Reconocimiento y pago de desequilibrio contractual por causa imputable a la Entidad. * Errores o imprecisiones en las actas de recibo parcial. * Adición de ítem no previsto sin estudio de mercado y/o con sobrecosto. * Mayores cantidades reconocidas y pagadas con valores unitarios superiores al pactado en el contrato. * Modificación contractual sin actualización de la garantía. * Inadecuada o inoportuna aplicación de facultad sancionatoria * Colapso o fallas en la estabilidad de la obra. * Incumplimiento de disposiciones ambientales y/o de la licencia ambiental. * Ejecución de un alcance inferior al contratado y pago total del contrato * No funcionalidad de lo ejecutado. * Bienes, servicios u obras inconclusas y/o que no brindan utilidad o beneficio. * Rendimientos financieros de recursos de anticipo o de cualquier recurso público no devueltos al tesoro público. |
| **Actividad de la Etapa Postcontractual** | * Inadecuada deducción de impuestos, tasas o contribuciones. * Pago de comisiones a éxito sin debida justificación. * Suscripción de acta de liquidación con imprecisiones de fondo * No amortización de anticipo * Suscripción de acta de liquidación sin el reconocimiento de sanciones impuestas. * Pérdida de competencia para liquidar por vencimiento del plazo legal, con saldos a favor de la Entidad. * Liquidación de mutuo acuerdo con recibo a satisfacción, habiendo imprecisiones o falsedades. * Deterioro del bien u obra por indebido mantenimiento. * Suscripción de acta de recibo final de obra con imprecisiones de fondo. |
| **Actividad de Manejo de bases de datos y sistemas de información.**  **(Gestión Humana/Nómina)** | * Bases de datos con falencias de información que genera pagos de subsidios u otros beneficios sin el cumplimiento de requisitos y condiciones. * Pago de subsidio u otros beneficios a personas fallecidas. * Pago de subsidios u otros beneficios a personas que no tienen derecho a los mismos a la luz de requisitos de ley. * Pago de subsidios por encima del beneficio otorgado. |
| **Actividad de la Gestión de Cobro.** | * Vencimiento de plazos para la labor de cobro. * Inadecuada gestión de cartera. |
| **Otras** |  |

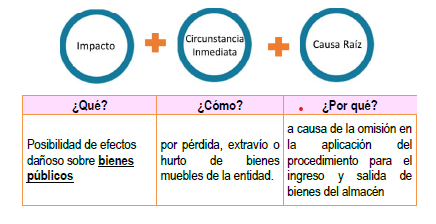
Fuente: Catálogo de puntos de Riesgo Fiscal – DAFP.

**Imagen No. 1. Estructura redacción de riesgo**

**a). Redacción Riesgos de Gestión (No Aplica para Riesgo Fiscal):**



**b). Redacción Riesgos de Gestión - FISCAL:**

**Fuente: Guía Administración de riesgos y diseño de controles – versión 6.0**

**c) Redacción Riesgo de Corrupción:**

**La Descripción del riesgo de corrupción debe incorporar los siguientes elementos:**

**ACCIÓN U OMISIÓN + USO DE PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO** + **EL BENEFICIO PROVADO:**

****

**d) Redacción Riesgo Seguridad de la Información:**

**Para cada riesgo se debe asociar el activo específico del proceso, identificar el riesgo de seguridad de la información: Pérdida de la confidencialidad – Pérdida de la Integridad y Pérdida de la disponibilidad y conjuntamente analizar las posibles amenazas y vulnerabilidades, ver siguiente cuadro:**

****

**Fuente: Guía Administración de riesgos y diseño de controles – versión 6.0**

**Tabla No. 5. Guía de Amenazas Comunes – Riesgos Seguridad de la Información**

| **Tipo** | **Amenaza** |
| --- | --- |
| Daño físico | Fuego |
| Agua |
| Contaminación |
| Accidente Importante |
| Destrucción del equipo o medios |
| Polvo, corrosión, congelamiento |
| Eventos naturales | Fenómenos climáticos |
| Fenómenos sísmicos |
| Fenómenos volcánicos |
| Fenómenos meteorológicos |
| Inundación |
| Perdida de los servicios esenciales | Fallas en el sistema de suministro de agua o aire acondicionado |
| Perdida de suministro de energía |
| Falla en equipo de telecomunicaciones |
| Perturbación debida a la radiación | Radiación electromagnética |
| Radiación térmica |
| Impulsos electromagnéticos |
| Compromiso de la información | Interceptación de señales de interferencia |
| comprometida |
| Espionaje remoto |
| Escucha encubierta |
| Hurto de medios o documentos |
| Hurto de equipo |
| Recuperación de medios reciclados o |
| desechados |
| Divulgación |
| Datos provenientes de fuentes no confiables |
| Manipulación con hardware |
| Manipulación con software |
| Detección de la posición |
| Fallas técnicas | Fallas del equipo |
| Mal funcionamiento del equipo |
| Saturación del sistema de información |
| Mal funcionamiento del software |
| Incumplimiento en el mantenimiento del |
| Sistema de información. |
| Acciones no autorizadas | Uso no autorizado del equipo /información |
| Copia fraudulenta del software |
| Uso de software falso o copiado |
| Corrupción de los datos |
| Procesamiento ilegal de datos |
| Compromiso de las funciones | Error en el uso |
| Falsificación de derechos |
| Abuso de derechos |
| Negación de acciones |
| Incumplimiento en la disponibilidad del personal |

**Fuente: ISO/IEC 27005:2009 y MINTIC guía de gestión de riesgos**

**Tabla No. 6. Acciones amenazantes (Amenaza Humana) – Riesgos Seguridad de la Información**

|  |  |  |
| --- | --- | --- |
| **Figura** | **Motivación** | **Acciones amenazantes** |
| Pirata informático, intruso ilegal | Reto | Piratería |
| Ego | Ingeniería Social |
| Rebelión | Intrusión en el sistema |
| Estatus | forzados al sistema |
| Dinero | Acceso no autorizado |
| Criminal de la computación | Destrucción información | Crimen por computador |
| Divulgación ilegal de la información | Acto fraudulento |
| Ganancia monetaria | Soborno de la información |
| Alteración autorizada datos | Suplantación de identidad |
| Terrorismo | Chantaje | Intrusión en el sistema |
| Destrucción | Bomba/Terrorismo |
| Explotación | Guerra de la información |
| Venganza | Ataques contra sistema DDoS |
| Ganancia política | Penetración sistema |
| Cubrimiento de los medios de comunicación | Manipulación sistema |
| Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses) | Ventaja competitiva | Ventaja de defensa |
| Espionaje económico | Hurto de información |
| Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos) | Curiosidad | Asalto a un empleado |
| Ganancia monetaria | Chantaje |

**Tabla No. 7. Guía de Vulnerabilidades comunes/causas – Riesgos Seguridad de la Información**

| **Tipo de activo** | **Vulnerabilidades** |
| --- | --- |
| **HARDWARE** | Mantenimiento insuficiente |
| Ausencia de esquemas de reemplazo periódico |
| Sensibilidad a la radiación electromagnética |
| Susceptibilidad a las variaciones de temperatura (al polvo o la suciedad) |
| Almacenamiento sin protección |
| Falta de cuidado en la disposición final |
| Copia no controlada |
| Ausencia de un eficiente control de cambios en la configuración |
| Susceptibilidad a las variaciones de voltaje |
| Susceptibilidad a las variaciones de temperatura |
| **SOFTWARE** | Ausencia o insuficiencia de pruebas de software |
| Ausencia de terminación de sesión |
| Ausencia de registros de auditoría |
| Asignación errada de los derechos de acceso |
| Interfaz de usuario compleja |
| Ausencia de documentación |
| Fechas incorrectas |
| Ausencia de mecanismos de identificación y autenticación de usuarios |
| Contraseñas sin protección |
| Software nuevo o inmaduro |
| Defectos bien conocidos en el software |
| Disposición o reutilización de los medios de almacenamiento sin borrado adecuado |
| Software de distribución amplia |
| En términos de tiempo utilización de datos errados en los programas de aplicación |
| Configuración incorrecta de parámetros |
| Tablas de contraseñas sin protección |
| Gestión deficiente de las contraseñas |
| Habilitación de servicios innecesarios |
| Especificaciones incompletas o no claras para los desarrolladores |
| Ausencia de control de cambios eficaz |
| Descarga y uso no controlado de software |
| Ausencia de copias de respaldo |
| Ausencia de protección física de la edificación, puertas y ventanas |
| Software obsoleto |
| Fallas en la producción de informes de gestión |
| **RED** | Ausencia de pruebas de envío o recepción de mensajes |
| Líneas de comunicación sin protección |
| Tráfico sensible sin protección |
| Conexión deficiente de los cables |
| Punto único de fallas |
| Ausencia de identificación y autentificación de emisor y receptor |
| Arquitectura insegura de la red |
| Transferencia de contraseñas en claro |
| Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento) |
| Conexiones de red pública sin protección |
| **PERSONAL** | Ausencia del personal |
| Entrenamiento insuficiente |
| Falta de conciencia en seguridad |
| Ausencia de políticas de uso aceptable |
| Trabajo no supervisado de personal externo o de limpieza |
| Procedimientos inadecuados de contratación |
| Uso incorrecto de software y hardware |
| Ausencia de mecanismos de monitoreo |
| **LUGAR** | Uso inadecuado de los controles de acceso al edificio y recintos |
| Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos |
| Áreas susceptibles a inundación |
| Red energética inestable |
| Ausencia de protección física de la edificación (Puertas y ventanas) |
| **ORGANIZACIÓN** | Ausencia de procedimiento de registro/retiro de usuarios |
| Ausencia de proceso para supervisión de derechos de acceso |
| Ausencia de control de los activos que se encuentran fuera de las instalaciones |
| Ausencia de acuerdos de nivel de servicio (ANS o SLA) |
| Ausencia de mecanismos de monitoreo para brechas en la seguridad |
| Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros). |
| Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad) |
| Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información |
| Ausencia de auditorias |
| Ausencia de procedimientos de identificación y valoración de riesgos |
| Ausencia de reportes de fallas en los registros de administradores y operadores |
| Respuesta inadecuada de mantenimiento del servicio |
| Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos |
| Ausencia de procedimientos de control de cambios |
| Ausencia de procedimiento formal para la autorización de la información disponible al público |
| Ausencia de asignación adecuada de responsabilidades en seguridad de la información |
| Ausencia de planes de continuidad |
| Ausencia de políticas sobre el uso de correo electrónico |
| Ausencia de procedimientos para introducción del software en los sistemas operativos |
| Ausencia de registros en bitácoras |
| Ausencia de procedimientos para el manejo de información clasificada |
| Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información |
| Ausencia de control de los activos que se encuentran fuera de las instalaciones |
| Ausencia de autorización de los recursos de procesamiento de información |
| Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad |
| Ausencia de revisiones regulares por parte de la Alta Dirección |
| Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales. |

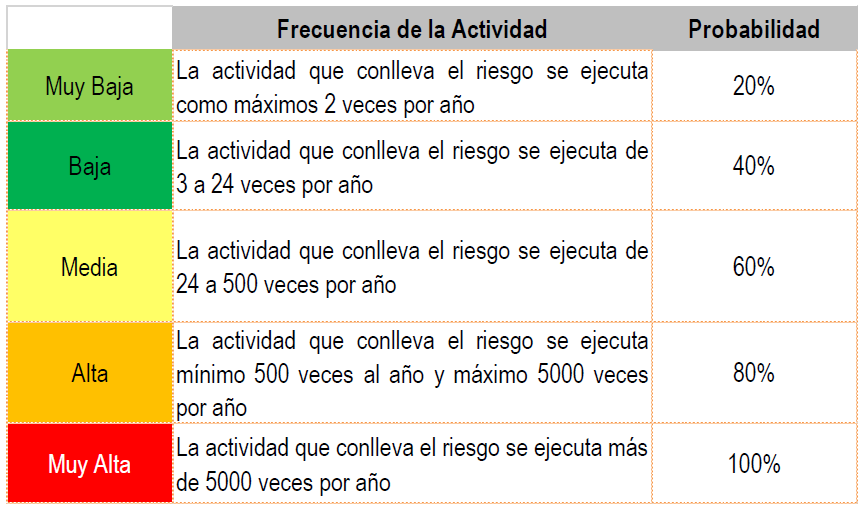
**Fuente: ISO/IEC 27005 Y MINTIC guía de gestión de riesgos**

1. **ANALISIS DEL RIESGOS**

Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto

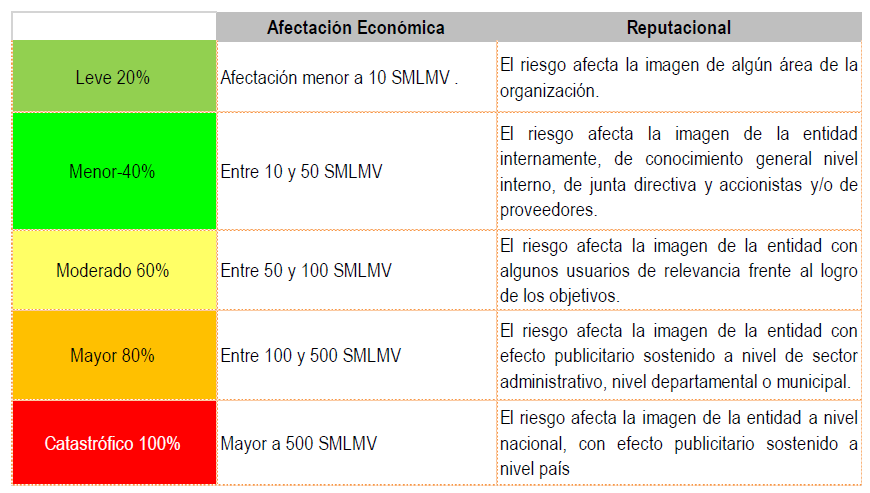
**Tabla No. 8 Criterios para definir el nivel de probabilidad**

Riesgos de Gestión incluido el riesgo fiscal y Seguridad de la Información

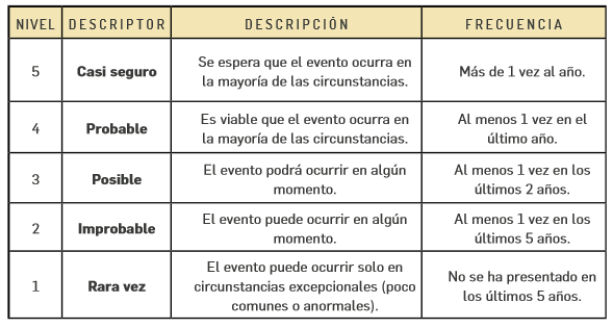


**Tabla No. 9. Criterios para definir el nivel de impacto**

Riesgos de Gestión incluido el riesgo fiscal y Seguridad de la Información



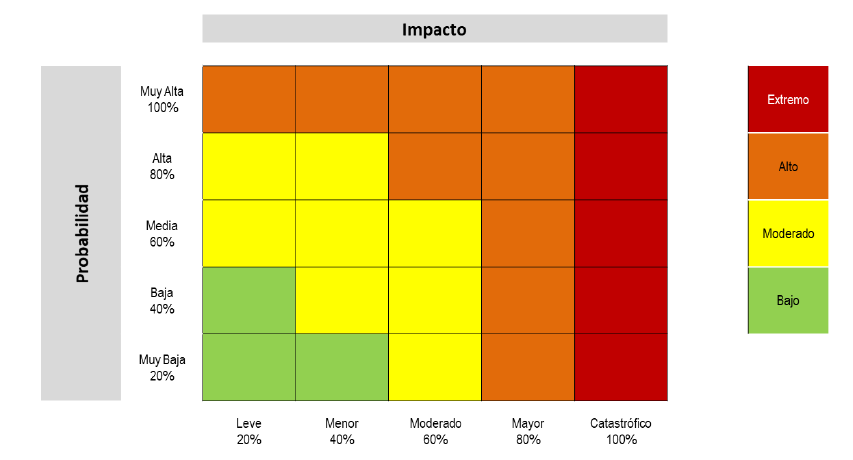
**Tabla No. 10 Criterios parar calificar la probabilidad - Riesgos de Corrupción**

**

**Tabla No. 11. Criterios para calificar el impacto- - Riesgos de Corrupción**



**Tabla No. 12. Zona de Riesgo - Matriz de calor**



1. **VALORACIÓN DE CONTROLES**

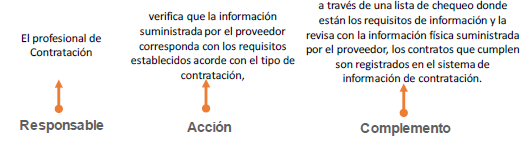
**Tabla No. 13. Ciclo del proceso y tipologías de controles**

Estructura descripción del Control:

Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

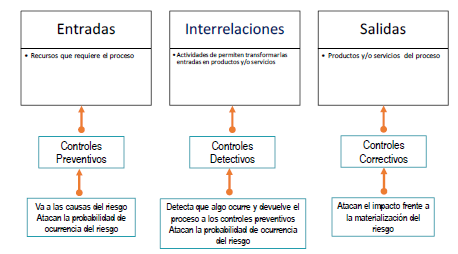
* **Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
* **Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.
* **Complemento**: corresponde a los detalles que permiten identificar claramente el objeto del control.

Ejemplo:



**Tipologías de Controles y los procesos:**

A través del ciclo de los procesos es posible establecer cuándo se activa un control y por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, en la figura 15 se consideran 3 fases globales del ciclo de un proceso así



**Tipologías de controles:**

Acorde con lo anterior, tenemos las siguientes tipologías de controles:

* **Control Preventivo:** Control accionado en la entrada del proceso y antes de que se realice la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles buscan establecer las condiciones que aseguren atacar la causa raíz y así evitar que el riesgo se concrete.
* **Control Detectivo:** Control accionado durante la ejecución de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo). Estos controles detectan el riesgo fiscal, pero generan reprocesos.
* **Control Correctivo:** Control accionado en la salida de la actividad en la que potencialmente se origina el riesgo fiscal (punto de riesgo) y después de que se materializa el riesgo fiscal.

Para el análisis y evaluación de los controles se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización.

**Ejemplo (Riesgo Fiscal):**

* **Proceso:** Gestión Administrativa y financiera.
* **Objetivo:** Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.
* **Alcance:** Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.
* **Punto de Riesgo:** Ingreso, custodia y salida de bienes muebles de la entidad
* **Riesgo Fiscal:** Posibilidad de efectos dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión en la aplicación del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte información a quien gestiona las pólizas cuando haya lugar (causa raíz).

**Controles identificados:**

* **Control Preventivo:** El jefe de almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable.
* **Control Detectivo:** El coordinador administrativo verifica mensualmente la relación de ingreso y salida de bienes muebles contra los inventarios generados por el sistema (actualización y ubicación en el inventario), en caso de encontrar inconsistencias solicita al Jefe de Almacén ubicar el bien faltante y realizar el ajuste, teniendo en cuenta los soportes de salida e ingreso del almacén.
* **Control Correctivo:** El director administrativo verifica la vigencia y actualización de la póliza de acuerdo a los bienes que ingresan a la entidad, en caso de presentarse un siniestro adelanta las reclamaciones respectivas ante el asegurador.

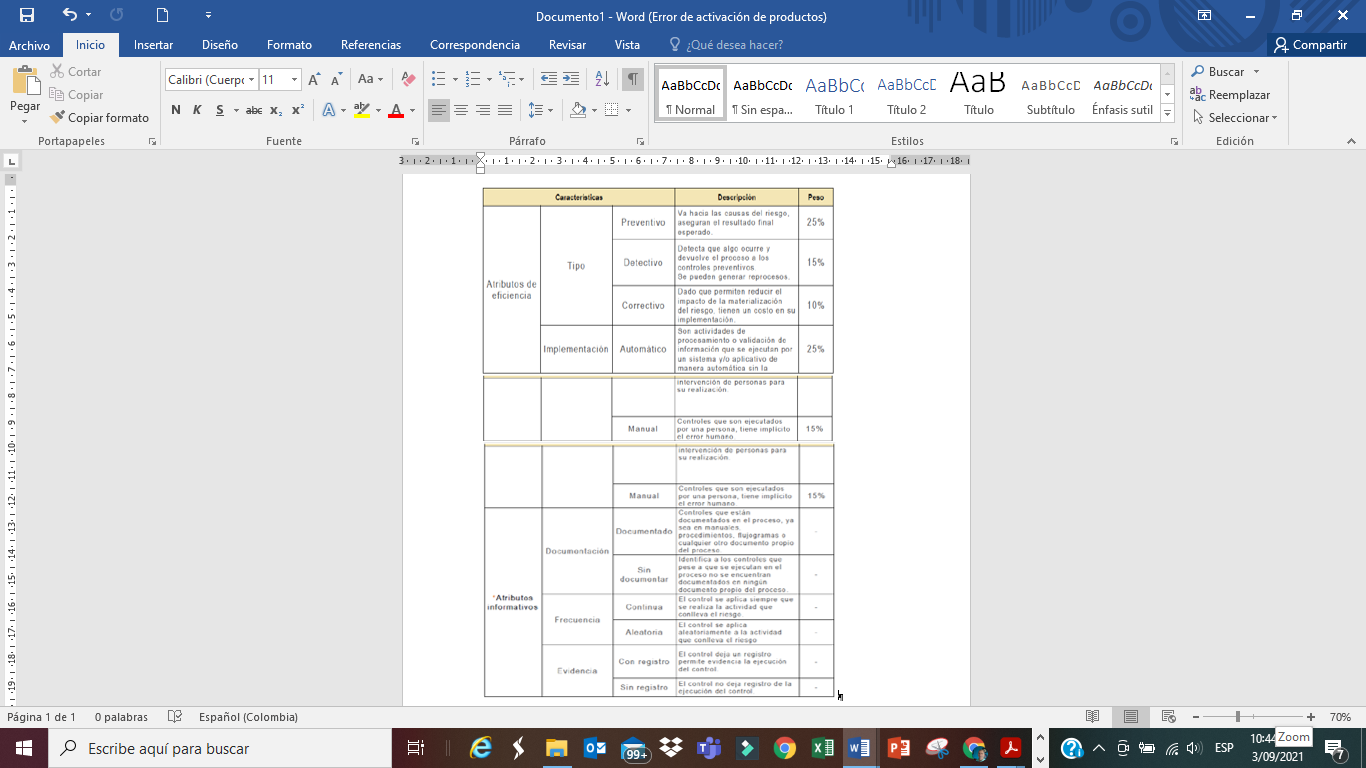
**Tabla No. 14**

**Anexo 4 “*Modelo Nacional de Gestión de riesgos de seguridad de la información en entidades públicas*”**

| **Controles de Seguridad de la Información**  **Fuente: ISO/IEC 27001:2013 - Anexo A - Controles** | | |
| --- | --- | --- |
| **5 - Políticas de seguridad** | A.5.1.1 Políticas para la seguridad de la información | Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes. |
| A.5.1.2 Revisión de las políticas para la seguridad de la información | Control: Las políticas para seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas. |
| **6. Organización de la seguridad de la información** | A.6.1.1 Roles y responsabilidades para la seguridad de la información | Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información. |
| A.6.1.2. Separación de deberes | Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización. |
| A.6.1.3. Contacto con las autoridades | Control: Se debe mantener los contactos apropiados con las autoridades pertinentes |
| A.6.1.4. Contacto con grupos de interés especial | Control: Se debe mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información y asociaciones de profesionales. |
| A.6.1.5 Seguridad de la información en gestión de proyectos | Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto. |
| A.6.2.1 Política para dispositivos móviles | Control: Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles. |
| A.6.2.2 Teletrabajo | Control: Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo. |
| **A.7 Seguridad de los recursos humanos** | A.7.1.1 Selección | Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos. |
| A.7.1.2 Términos y condiciones del empleo | Control: Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información. |
| A.7.2.1 Responsabilidades de la dirección | Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo  con las políticas y procedimientos establecidos por la organización. |
| A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información | Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo. |
| A.7.2.3 Proceso disciplinario | Control: Se debe contar con un proceso disciplinario formal el cual debe ser comunicado, para emprender acciones contra empleados hayan cometido una violación a la seguridad de la información. |
| A.7.3.1 Terminación o cambio de responsabilidades de empleo | Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se debe definir, comunicar al empleado o contratista y hacer cumplir. |
| **A.8 Gestión de activos** | A.8.1.1 Inventario de activos | Control: Se debe identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se deber elaborar y mantener un inventario de estos activos. |
| A.8.1.2 Propiedad de los activos | Control: Los activos mantenidos en el inventario deben tener un propietario. |
| A.8.1.3 Uso aceptable de los activos | Control: Se debe identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información. |
| A.8.1.4 Devolución de activos | Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo. |
| A.8.2.1 Clasificación de la información | Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. |
| A.8.2.2 Etiquetado de la información | Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización. |
| A.8.2.3 Manejo de activos | Control: Se debe desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización. |
| A.8.3.1 Gestión de medios removibles | Control: Se debe implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización. |
| A.8.3.2 Disposición de los medios | Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales. |
| A.8.3.3 Transferencia de medios físicos | Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte. |
| **A.9 Control de acceso** | A.9.1.1 Política de control de acceso | Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información |
| A.9.1.2 Acceso a redes y a servicios en red | Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente. |
| A.9.2.1 Registro y cancelación del registro de usuarios | Control: Se debe implementar un proceso formal de registro y de cancelación de usuarios, para posibilitar la asignación de los derechos de acceso. |
| A.9.2.2 Suministro de acceso de usuarios | Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios. |
| A.9.2.3 Gestión de derechos de acceso privilegiado | Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. |
| A.9.2.4 Gestión de información de autenticación secreta de usuarios | Control: La asignación de la información secreta se debe controlar por medio de un proceso de gestión formal. |
| A.9.2.5 Revisión de los derechos de acceso de usuarios | Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares. |
| A.9.2.6 Retiro o ajuste de los derechos de acceso | Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se debe ajustar cuando se hagan cambios. |
| A.9.3.1 Uso de la información de autenticación secreta | Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta |
| A.9.4.1 Restricción de acceso Información | Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se deben restringir de acuerdo con la política de control de acceso. |
| A.9.4.2 Procedimiento de ingreso seguro | Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro. |
| A.9.4.3 Sistema de gestión de contraseñas | Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas |
| A.9.4.4 Uso de programas utilitarios privilegiados | Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones. |
| A.9.4.5 Control de acceso a códigos fuente de programas | Control: Se deben restringir el acceso a los códigos fuente de los programas. |
| **A.10 Criptografía** | A.10.1.1 Política sobre el uso de controles criptográficos | Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. |
| A.10.1.2 Gestión de llaves | Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida. |
| **A.11 Seguridad física y del entorno** | A.11.1.1 Perímetro de seguridad física | Control: Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información. |
| A.11.1.2 Controles de Acceso físicos | Control: Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado. |
| A.11.1.3 Seguridad de oficinas, recintos e instalaciones | Control: Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones. |
| A.11.1.4 Protección contra amenazas externas y ambientales | Control: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. |
| A.11.1.5 Trabajo en áreas seguras | Control: Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras. |
| A.11.1.6 Áreas de despacho y carga | Control: Se debe controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado. |
| A.11.2.1 Ubicación y protección de los equipos | Control: Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado. |
| A.11.2.2 Servicios de suministro | Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. |
| A.11.2.3 Seguridad del cableado | Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debe estar protegido contra interceptación, interferencia o daño |
| A.11.2.4 Mantenimiento de equipos | Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas. |
| A.11.2.5 Retiro de activos | Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa |
| A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones | Control: Se debe aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones. |
| A.11.2.7 Disposición segura o reutilización de equipos | Control: Se debe verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización. |
| A.11.2.8. Equipos de usuario desatendidos | Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada. |
| A.11.2.9 Política de escritorio limpio y pantalla limpia | Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información. |
| **A.12 Seguridad de las operaciones** | A.12.1.1 Procedimientos de operación documentados | Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten. |
| A.12.1.2 Gestión de cambios | Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información. |
| A.12.1.3 Gestión de capacidad | Control: Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura. |
| A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación | Control: Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación. |
| A.12.2.1 Controles contra códigos maliciosos | Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos. |
| A.12.3.1 Respaldo de información | Control: Se deben hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada. |
| A.12.4.1 Registro de eventos | Control: Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información. |
| A.12.4.2 Protección de la información de registro | Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado. |
| A.12.4.3 Registros del administrador y del operador | Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad. |
| A.12.4.4 sincronización de relojes | Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo |
| A.12.5.1 Instalación de software en sistemas operativos | Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos. |
| A.12.6.1 Gestión de las vulnerabilidades técnicas | Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. |
| A.12.6.2 Restricciones sobre la instalación de software | Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios. |
| A.12.7.1 Información controles de auditoría de sistemas | Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio. |
| **A.13 Seguridad de las comunicaciones** | A.13.1.1 Controles de redes | Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones. |
| A.13.1.2 Seguridad de los servicios de red | Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente. |
| A.13.1.3 Separación en las redes | Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes. |
| A.13.2.1 Políticas y procedimientos de transferencia de información | Control: Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación. |
| A.13.2.2 Acuerdos sobre transferencia de información | Control: Los acuerdos deben tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas. |
| A.13.2.3 Mensajería electrónica | Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica. |
| A.13.2.4 Acuerdos de confidencialidad o de no divulgación | Control: Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información. |
| **A.14 Adquisición, desarrollo y mantenimientos de sistemas** | A.14.1.1 Análisis y especificación de requisitos de seguridad de la información | Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes. |
| A.14.1.2 Seguridad de servicios de las aplicaciones en redes publicas | Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas. |
| A.14.1.3 Protección de transacciones de los servicios de las aplicaciones | Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada. |
| A.14.2.1 Política de desarrollo seguro | Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización. |
| A.14.2.2 Procedimientos de control de cambios en sistemas | Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos  formales de control de cambios. |
| A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación | Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización. |
| A.14.2.4 Restricciones en los cambios a los paquetes de software | Control: Se debe desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente. |
| A.14.2.5 Principios de construcción de sistemas seguros | Control: Se debe establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información. |
| A.14.2.6 Ambiente de desarrollo seguro | Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas. |
| A.14.2.7 Desarrollo contratado externamente | Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente. |
| A.14.2.8 Pruebas de seguridad de sistemas | Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad |
| A.14.2.9 Prueba de aceptación de sistemas | Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados. |
| A.14.3.1 Protección de datos de prueba | Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente. |
| **A.15 Relación con los proveedores** | A.15.1.1 Política de seguridad de la información para las relaciones con proveedores | Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar. |
| A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores | Control: Se debe establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización. |
| A.15.1.3 Cadena de suministro de tecnología de información y comunicación | Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación. |
| A.15.2.1 Seguimiento y revisión de los servicios de los proveedores | Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores. |
| A.15.2.2 Gestión de cambios en los servicios de proveedores | Control: Se debe gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos. |
| **A.16 Gestión de incidentes de seguridad de la información** | A.16.1.1 Responsabilidades y procedimientos | Control: Se debe establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. |
| A.16.1.2 Reporte de eventos de seguridad de la información | Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible. |
| A.16.1.3 Reporte de debilidades de seguridad de la información | Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios. |
| A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos | Control: Los eventos de seguridad de la información se deben evaluar y se deben decidir si se van a clasificar como incidentes de seguridad de la información. |
| A.16.1.5 Respuesta a incidentes de seguridad de la información | Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados. |
| A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información | Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros. |
| A.16.1.7 Recolección de evidencia | Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia. |
| **A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio** | A.17.1.1 Planificación de la continuidad de la seguridad de la información | Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre. |
| A.17.1.2 Implementación de la continuidad de la seguridad de la información | Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para  asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa. |
| A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información | Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas. |
| A.17.2.1 Disponibilidad de instalaciones de procesamiento de información. | Control: Las instalaciones de procesamiento de información se debe implementar con redundancia suficiente para cumplir los requisitos de disponibilidad. |
| **A.18 Cumplimiento** | A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales | Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización. |
| A.18.1.2 Derechos de propiedad intelectual | Control: Se debe implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. |
| A.18.1.3 Protección de registros | Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio. |
| A.18.1.4 Privacidad y protección de datos personales | Control: Cuando sea aplicable, se debe asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes |
| A.18.1.5 Reglamentación de controles criptográficos | Control: se debe usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes |
| A.18.2.1 Revisión independiente de la seguridad de la información | Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos. |
| A.18.2.2 Cumplimiento con las políticas y normas de seguridad | Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad. |
| A.18.2.3 Revisión del cumplimiento técnico | Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información. |

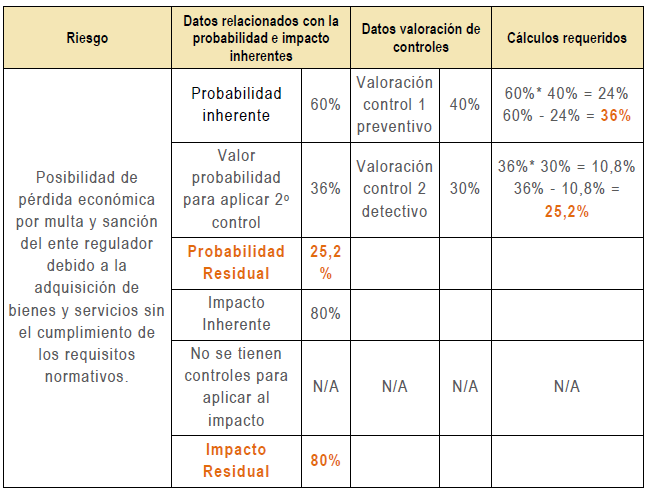
**Tabla No. 15. Atributos para el diseño de controles -**

Riesgos de Gestión y Seguridad de la Información



**Tabla No. 16. Ejemplo aplicación de controles para establecer el riesgo residual**

Riesgos de Gestión y Seguridad de la Información



**Valoración de Controles Riesgos de Corrupción (Tablas 17-22)**

**Tabla No. 17. Peso de cada variable en el Diseño del Control para la Mitigación del Riesgo**



**Tabla No. 18. Calificación diseño del control**

|  |  |
| --- | --- |
| Rango de calificación del diseño del control | Resultado - peso en la evaluación del diseño del control |
| Fuerte | Calificación entre 96 y 100 |
| Moderado | Calificación entre 86 y 95 |
| Débil | Calificación entre 0 y 85 |

**Tabla No. 19. Calificación ejecución del control**

|  |  |
| --- | --- |
| **Rango de calificación de la ejecución del control** | **Resultado - peso en la evaluación de la ejecución del control** |
| Fuerte | El control se ejecuta de manera consistente por parte del responsable. |
| Moderado | El control se ejecuta algunas veces por parte del responsable. |
| Débil | El control no se ejecuta por parte del responsable. |

**Tabla No. 20. Calificación Solidez Individual del Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Peso individual del diseño (DISEÑO)** | **El control se ejecuta de manera consistente por los responsables. (EJECUCIÓN)** | **Solidez individual de cada control  fuerte:100  moderado:50  debil:0** | **Aplica plan de acción para fortalecer el control Sí / NO** |
| fuerte calificación entre 96 y 100 | fuerte (siempre se ejecuta) | fuerte + fuerte = fuerte | No |
| moderado (algunas veces) | fuerte + moderado = moderado | Si |
| débil (no se ejecuta) | fuerte + débil = débil | Si |
| moderado calificación entre 86 y 95 | fuerte (siempre se ejecuta) | moderado + fuerte = moderado | Si |
| moderado (algunas veces) | moderado + moderado = moderado | Si |
| débil (no se ejecuta) | moderado + débil = débil | Si |
| débil entre 0 y 85 | fuerte (siempre se ejecuta) | débil + fuerte = débil | Si |
| moderado (algunas veces) | débil + moderado = débil | Si |
| débil (no se ejecuta) | débil + débil = débil | Si |

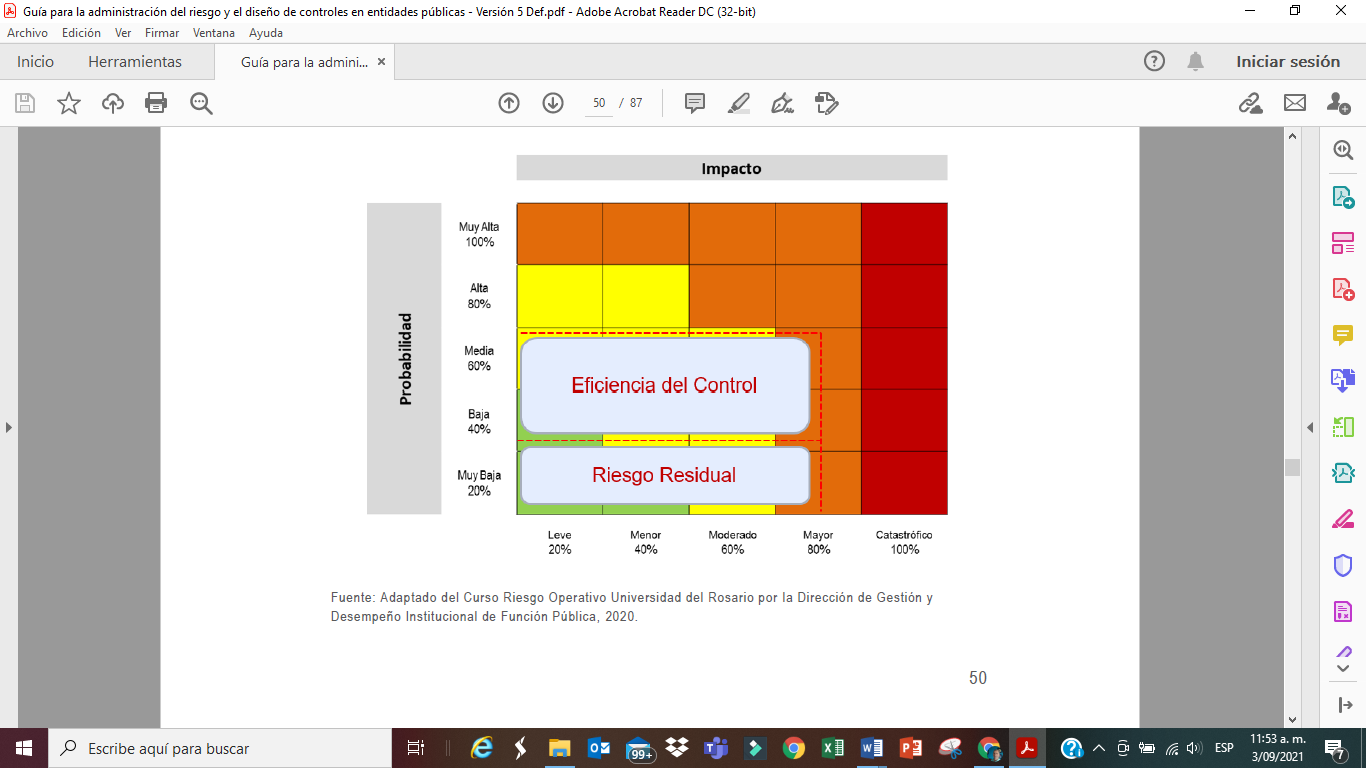
**Tabla No. 21. Calificación de la Solidez del Conjunto de Controles**

|  |  |
| --- | --- |
| Fuerte | El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100. |
| Moderado | El promedio de la solidez individual de cada control al sumarlos y ponderarlos la calificación está entre 50 y 99 |
| Débil | El promedio de la solidez individual de cada control al sumarlos y ponderarlos la calificación es menor a 50. |

**Tabla No. 22. Resultados Posibles desplazamientos Probabilidad e Impacto**

| **Solidez del conjunto de los controles** | **Controles ayudan a disminuir la probabilidad** | **Controles ayudan a disminuir impacto** | **# Columnas en la matriz de riesgo que se desplaza en el eje de la probabilidad** | **# Columnas en la matriz de riesgo que se desplaza en el eje de impacto** |
| --- | --- | --- | --- | --- |
| fuerte | directamente | directamente | 2 | 2 |
| fuerte | directamente | Indirectamente | 2 | 1 |
| fuerte | directamente | no disminuye | 2 | 0 |
| fuerte | no disminuye | directamente | 0 | 2 |
| moderado | directamente | directamente | 1 | 1 |
| moderado | directamente | Indirectamente | 1 | 0 |
| moderado | directamente | no disminuye | 1 | 0 |
| moderado | no disminuye | directamente | 0 | 1 |

Tabla No. 23. Movimiento en la Matriz de Calor



Fecha aprobación modificación: Memorando 3-2024-14231 del 11/06/2024