# MATRIZ DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

| | |
|---|---|
| **OBJETIVO** | Identificar y mitigar con precisión y eficacia los riesgos de seguridad y privacidad de la información para asegurar la protección continua de los datos de la entidad |
| **ALCANCE** | A toda la organización |

| RIESGO | | | | | | | | | | | | | | | | | | CONTROLES DEL RIESGO | | | | RIESGO RESIDUAL | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ID** | **Código** | **Fecha Identificación** | **Nombre** | **Descripción** | **Factores** | **Responsable** | **Sedes** | **Procesos** | **Categoría** | **Fuente de identificación (Nuevos riesgos)** | **Fuente de materialización (riesgos materializados)** | **Causas** | **PROBABILIDAD** | **IMPACTO** | **Impacto Economico** | **Impacto reputacional** | **Probabilidad** | **Impacto** | **Zona inherente** | **ID** | **Código** | **Nombre** | **Probabilidad Residual** | **Impacto Residual** | **Zona Residual** |
| 81 | | 2020-12-03 | Generación de vulnerabilidades en la infraestructura tecnológica por Incumplimiento de los procedimientos en el manejo de los Sistemas de información | Posibilidad de vulnerabilidad en la infraestructura debido a desconocimiento respecto al manejo de los Sistemas de información de la entidad, por parte de los funcionarios/ contratistas en el desarrollo de sus funciones, lo cual genera vulnerabilidades en la infraestructura tecnológica y retrasos en la operación e implementación de los procesos. | | Profesional Universitario G2 - Oficina Estrategia (TI) | - SEDE PRINCIPAL CIUDAD DEL RÍO | - Gestion de Tecnologia de la Informacion | | | | - Carencia de capacitaciones sobre el buen manejo de los sistemas de información (Origen: Interno \| Factor: Procesos)<br>- phishing (Origen: Interno \| Factor: Tecnologias de la Información)<br>- Acceso no autorizado servidor (Origen: Interno \| Factor: Tecnologias de la Información) | Muy Baja | Moderado | Moderado | Moderado | 20 | 60 | Moderado | 528<br>529<br>530 | | Capacitar en politica de seguridad de la información.<br>Inducción nuevos funcionarios y contratistas<br>Documento de clasificación de información Publica Reservada | 4 | 60 | Moderado |
| 143 | | 2020-12-03 | Afectaciones económicas y reputacionales por la materialización de ataque informático. | Posibilidad de afectación economica y reputacional debido a materialización de ataques informáticos | | Profesional Universitario G2 - Oficina Estrategia (TI) | - SEDE PRINCIPAL CIUDAD DEL RÍO | - Gestion de Tecnologia de la Informacion | - Fallas tecnológicas | | | - Falencias en la implementación de las políticas de seguridad y privacidad de la información (Origen: Interno \| Factor: Estrategia) | Muy Baja | Mayor | Mayor | Mayor | 20 | 80 | Alto | 509<br>531<br>537<br>638 | | Capacitar en politica de seguridad de la información.<br>Control documento de clasificación de información Publica Reservada<br>Ataque informático<br>Ataque informático | 3 | 80 | Alto |
| 144 | | 2020-12-03 | Afectación reputacional y/o económica por Interrupción de la Operación de la Plataforma Tecnológica. | Se pueden presentar situaciones externas que afecten la operación de la plataforma tecnológica de la Entidad, como desastres naturales, atentados terroristas, fallas en el proveedor de servicios informÁticos. Al interior de la Entidad se pueden presentar interrupciones debido a la manipulación indebida e incorrecta de la infraestructura tecnológica. | | Profesional Universitario G2 - Oficina Estrategia (TI) | - SEDE PRINCIPAL CIUDAD DEL RÍO | - Gestion de Tecnologia de la Informacion | - Fallas tecnológicas<br>- Fraude interno<br>- Relaciones laborales | | | - Intermitencias en la disponibilidad de los servicios de la infraestructura tecnológica de la entidad (Origen: Interno \| Factor: Tecnologias de la Información) | Muy Baja | Menor | Menor | Menor | 20 | 40 | Bajo | 510<br>532<br>533 | | Aplicar procedimientos de seguridad de la información.<br>Control documento de clasificación de información Publica Reservada<br>Check List revisión de infraestructura | 4 | 40 | Bajo |
| 145 | | 2020-12-03 | Pérdida, alteración o sustracción de Información en medio magnético o físico. | Este riesgo hace referencia a la posibilidad que puede tener un usuario de realizar procedimientos por fuera de sus autorizaciones o perfiles, de manera intencionada o no, para modificar, sustraer o eliminar Informacion obtenida en medios magnéticos o físicos. | | Profesional Universitario G2 - Oficina Estrategia (TI) | - SEDE PRINCIPAL CIUDAD DEL RÍO | - Gestion de Tecnologia de la Informacion | | | | - Configuración errónea de los perfiles de cada usuario (Origen: Interno \| Factor: Tecnologias de la Información) | Muy Baja | Menor | Menor | Menor | 20 | 40 | Bajo | 511<br>534<br>535<br>536<br>537<br>639 | | Realizar copias de seguridad<br>Control documento de clasificación de información Publica Reservada<br>Check List revisión de infraestructura<br>control de acceso limitado de acuerdo con las funciones<br>Bloqueo de medios físicos<br>Pérdida, alteración o sustracción de Información en medio magnético o físico. | 1 | 40 | Bajo |
| 146 | | 2020-12-03 | Alteración, divulgación o uso mal intencionado de información sensible para la Entidad | Se debe resguardar la información del uso mal intencionado referente a posibles actos desleales, incumplimiento de procedimientos, aplicacion inadecuada de controles y/o interrupcion de los servicios prestados por terceros. | | Profesional Universitario G2 - Oficina Estrategia (TI) | - SEDE PRINCIPAL CIUDAD DEL RÍO | - Gestion de Tecnologia de la Informacion | | | | - Configuración errónea de los perfiles de cada usuario (Origen: Interno \| Factor: Tecnologias de la Información) | Muy Baja | Menor | Menor | Menor | 20 | 40 | Bajo | 512<br>538<br>633<br>640 | 146 | Aplicar al control de permisos por usuario<br>acuerdo de confidencialidad de la información<br>Alteración, divulgación o uso mal intencionado de información sensible para la Entidad<br>Alteración, divulgación o uso mal intencionado de información sensible para la Entidad | 3 | 40 | Bajo |
| 176 | | | Riesgo de filtración de información sensible: Pérdida de confianza, daño a la reputación y pérdida de ventaja competitiva | Riesgo de filtración de información sensible: Posibilidad de que información confidencial de la compañía y sus clientes sea divulgada, lo que podría ocasionar pérdida de confianza, daño a la reputación y pérdida de competitividad en el mercado. | | Profesional Universitario G2 - Oficina Estrategia (TI) | - SEDE PRINCIPAL CIUDAD DEL RÍO | - Planeacion Estratégica | | | | - Falencias en la implementación de las políticas de seguridad y privacidad de la información (Origen: Interno \| Factor: Tecnologias de la Información) | Media | Menor | Menor | Menor | 60 | 40 | Moderado | 653 | | Blindar los datos solo a partes interesadas, en procesos de información reservada | 35 | 40 | Moderado |