MATRIZ DE RIESGOS PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023

EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE MANIZALES – ERUM S.A.S.

Manizales, Centro Administrativo Municipal CAM
Calle 19 #21 - 44 Torre A pisos 7 y 13
Tels: (+57) 6 8722053• (+57) 6 8720538 • (+57) 6 8720630
contacto@erum.gov.co • www.erum.gov.co

IDENTIFICACIÓN DEL RIESGOS

La identificación del riesgo permite conocer los incidentes que puedan causar las alteraciones en el funcionamiento de la entidad, y pueden comprometer y afectar la confidencialidad, integridad y disponibilidad de la información.

El propósito principal de identificar el riesgo es determinar que puede suceder en el caso de tener una perdida potencial de información y que acciones tomar al comprender el cómo, dónde y por qué puede ocurrir el evento.

Riesgos	Causas	Efectos
Pérdida, Robo o Fuga de Información.	● Fallas en el proceso del respaldo de la información o restauración de la misma. ● Fallas en los análisis y socialización de las vulnerabilidades de la infraestructura de TI. ● Falta de políticas en el manejo de la información de los empleados. ● Falta de control en el acceso de red a equipos no autorizados. ● Ataques externos a la red de datos. ● Falta de capacitaciones a empleados en temas de seguridad de los datos. ● Acceso de personal no autorizado a los equipos de la entidad. ● No cerrar las sesiones o bloquear accesos a equipos y aplicaciones al momento de retirarse del equipo. ● Acceso no autorizado a las oficinas o dependencias.	● Fugas de información. ● Vulnerabilidad en los sistemas. ● Pérdidas económicas. ● Daño a infraestructura TI.
Correos electrónicos no seguros.	● Desconocimiento de los riesgos al acceder a correos falsos. ● Fallas en los filtros de seguridad o mala configuración del servidor. ● Falta de Programas de DLP (Data Lost Prevention). Falta de instalación de EndPoint	● Instalación de programas espías. ● Robo de documentos.

	(programa seguridad punto final) en las estaciones de trabajo.	
Daño en los equipos tecnológicos.	● Falta de mantenimiento. ● Mal uso de las herramientas tecnológicas. ● Malas conexiones eléctricas.	● Pérdida de información. ● Deterioro de los equipos. ● Causa de incendio en las instalaciones.
Pérdida de la conexión.	● Daños en el proveedor ISP (Internet Service Provider). ● Ataque DDoS o DOS (denegación de servicios distribuidos o Denegación de servicios)	● Pérdida económica.

IDENTIFICACIÓN DE LAS AMENAZAS

Las amenazas causan daños a los activos como información, procesos y sistemas lo que afecta a cualquier entidad. Estas amenazas pueden ser naturales o humanas, por lo que pueden ser accidentales o deliberadas. Estas amenazas se deberían identificar genéricamente y por tipo.

Tipo	Amenaza
Eventos naturales	Fenómenos Climáticos, polvo, corrosión
Daño físico	Pérdida del suministro de energía
Acciones no autorizadas	Uso no autorizado del equipo
	Corrupción de datos
	Procesamiento ilegal de datos
	Acceso forzado al sistema
Pérdida de los servicios esenciales	Falla del sistema de aire acondicionado
	Falla en equipos de comunicaciones
	Fallos en discos de datos
Compromiso de la información	Hurto de documentos
	Hurto de equipos de computo
Fallas técnicas	Fallas en equipos
	Fallas en el diseño de software
	Faltas de mantenimiento
Acciones no autorizadas	Uso no autorizado de equipos
	Copias ilegales de software y datos reservados

IDENTIFICACIÓN DE LAS VULNERABILIDADES

Las vulnerabilidades son las debilidades que se encuentran en un activo o en un control y se pueden explotar por una o más amenazas, lo que lo convierte en un riego de seguridad.

Para proteger la información, se debe identificar, valorar, priorizar y corregir las debilidades que sean identificadas en los activos.

Tipo de activo	Vulnerabilidades	Descripción
HARDWARE	Fácil acceso a las dependencias de la entidad.	No existen controles para filtrar el acceso a los visitantes y/o funcionarios de otras dependencias.
	Falta de sistemas biométricos para acceso a dependencias que manejan información clasificada y reservada.	Estos dispositivos reducen el riesgo de acceder a lugares con información reservada o clasificada, llevando el control de usuarios.
SOFTWARE	Interfaz de usuario compleja	Genera errores en el uso de los aplicativos.
	Ausencia de documentación	No existen manuales para el uso de los aplicativos.
	Mala parametrización	Conlleva a generar errores en el registro de los datos.
	Contraseñas simples	Los aplicativos permiten claves simples, lo que genera riesgo de acceso fácil al sistema.
RED	Cables con conexiones deficientes.	Generan fallas en la entrega de los datos.
ORGANIZACION	No existen políticas de Escritorio Limpio.	Se deben implementar políticas, que generen conciencia en los funcionarios sobre la importancia de no dejar expuesto al momento de retirarse del lugar de trabajo, sesiones abiertas, documentos y objetos de valor.
PERSONAL	Documentos en la papelera completos.	Se deben destruir los documentos que se desechan, para no comprometer datos confidenciales.
	Falta de capacitaciones a funcionarios sobre la seguridad informática.	Es de gran importancia capacitar a los funcionarios, quienes son los que se exponen ante los riesgos de

		posibles ataques y con las suficientes bases pueden mitigarlos.
	Fallas en las copias de seguridad.	Importante capacitar a los funcionarios sobre cómo hacer copias de sus datos y con qué periodicidad.

IDENTIFICACIÓN DE CONTROLES EXISTENTES

Evaluación del Riesgo

La evaluación del riesgo se hace de manera cualitativa, generando una comparación, donde se obtiene como resultado el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo la matriz denominada "Matriz de calificación, evaluación y respuesta a los riesgos".

TABLA DE PROBABILIDAD			
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**	**FRECUENCIA**
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos una vez en los últimos 5 años.
3	Posible	El evento podría ocurrir en algún momento.	Al menos una vez en los últimos 2 años.
4	Probable	El evento probablemente ocurra en la mayoría de las circunstancias.	Al menos una vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de una vez al año.

TABLA DE IMPACTO		
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efecto mínimo sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto mínimos sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efecto sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

TRATAMIENTO DEL RIESGO

La Empresa de Renovación y Desarrollo urbano de Manizales debe definir las siguientes opciones para tratar los riesgos:

Evitar el riesgo

- Esta opción de tratamiento busca eliminar la probabilidad de ocurrencia o el impacto del riesgo.
- Tomar las medidas necesarias para prevenir la materialización del riesgo. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.
- Se implementa cuando el riesgo se puede tratar internamente y puede llevarse a un nivel aceptable.
- Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección).

Transferir todo o parte del riesgo

- Requiere hacer un traslado a terceros u otras organizaciones parte del impacto negativo de una amenaza, como contratos a riesgo compartido.
- Al transferir el riesgo a un tercero le damos la responsabilidad para su administración, pero no significa que eliminamos el riesgo.

Asumir el riesgo

- residual que se mantiene, en este caso, el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

La Empresa de Renovación y Desarrollo urbano de Manizales, realizará evaluaciones al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, por medio de monitoreos, revisando que los procesos se lleven acorde a las implementaciones necesarias, al menos entre periodos de 6 meses, 1 año o cuando sea necesario. Los procesos de evaluación y monitoreo deben estar apoyados en los líderes de la Oficina de Control Interno en coordinación con la Oficina de Comunicaciones.