FORMULARIO DE EVALUACIÓN DE RIESGOS

1. Información General

Nombre de la organización: Unidad de Gestión General (UGG)

Fecha de evaluación de riesgos:

Versión del documento: 1.0

Departamento/Unidad Evaluada:

2. Descripción del Riesgo

ID del Riesgo	Descripción del Riesgo	Probabilidad	Impacto	Nivel de Riesgo (Bajo/Medio/Alto)
R1	Acceso no autorizado a información clasificada	Alta	Alto	Alto
R2	Ciberataques a la infraestructura tecnológica (phishing, ransomware)	Media	Alto	Medio
R3	Fugas de datos sensibles debido a la falta de control en la gestión de accesos	Alta	Alto	Alto

3. Análisis del Riesgo

ID del Riesgo	Causa raíz del Riesgo	Consecuencias	Controles Existentes	Controles Propuestos
R1	Deficiencias en el control de acceso a sistemas críticos.	Exposición de datos sensibles, daños a la integridad de la información, impacto en la reputación.	Autenticación básica, acceso por roles.	Implementación de autenticación multifactor, revisión periódica de accesos.
R2	Ataques de malware dirigidos por actores maliciosos.	Pérdida de datos, interrupción de servicios críticos.	Antivirus, firewalls.	Implementación de herramientas avanzadas de detección y respuesta ante amenazas (EDR).
R3	Falta de políticas claras en la gestión de contraseñas y accesos.	Accesos no autorizados, filtración de información.	Políticas de contraseñas, control de accesos por roles.	Capacitación en seguridad para empleados, uso de contraseñas complejas y gestión segura.

4. Evaluación y Tratamiento de Riesgos				
D del Riesgo	**Nivel de Riesgo Inicial (Bajo/Medio/Alto)**	**Tratamiento Propuesto**	**Control de Mitigación Implementado**	**Nivel de Riesgo Residual (Bajo/Medio/Alto)**
R1	Alto	Implementar controles más estrictos de acceso a información clasificada y auditorías frecuentes.	Implementación de control de acceso basado en roles y multifactor.	Bajo
R2	Medio	Mejorar las defensas contra ciberataques con una solución avanzada de detección de intrusos.	Instalar una solución de detección y respuesta a intrusiones.	Bajo
R3	Alto	Realizar auditorías periódicas de accesos y gestión de contraseñas.	Establecer políticas claras y formación continua en seguridad.	Medio

5. Plan de Acción				
ID del Riesgo	**Acción Correctiva/Preventiva Propuesta**	**Responsable**	**Fecha de Implementación**	**Estado (Pendiente/En Proceso/Completado)**
R1	Implementación de autenticación multifactor en todos los sistemas críticos.	Equipo de TI		En Proceso
R2	Instalación de solución avanzada de detección de amenazas.	Seguridad Informática		Pendiente
R3	Capacitación a todos los empleados sobre el manejo de contraseñas y acceso.	Recursos Humanos		Completado

Nombre del Responsable	Firma	Fecha de Aprobación