MATRIZ DE RIESGOS SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN - SGSI

Código:
Versión: 01
Pagina: Ver (Pie de pagina)

ACTIVO	IDENTIFICADOR DE RIESGO	RIESGO	CAUSA	EFECTO - CONSECUENCIA	RIESGO INHERENTE: PROBABILIDAD	RIESGO INHERENTE: IMPACTO	RIESGO INHERENTE: VALOR (P x I) (INFORMACIÓN ANTES DE CONTROLES)	CRITERIOS ERCA (Evitar, Reducir, Compartir, Asumir)	CONTROLES	TIPO DE CONTROL	EVALUACIÓN DEL RIESGO RESIDUAL: HERRAMIENTAS PARA EJERCER CONTROL	MANUALES, INSTRUCTIVOS O PROCEDIMIENTOS	EFECTIVIDAD DEL CONTROL	RESPONSABLES DEL CONTROL Y SEGUIMIENTO	EL CONTROL ES AUTOMATICO	EI CONTROL ES MANUAL	FRECUENCIA DE EJECUCIÓN DEL CONTROL Y SEGUIMIENTO	PONDERACIÓN DE CONTROLES	TOTAL DE LA PONDERACIÓN DEL RIESGO	RIESGO RESIDUAL: PROBABILIDAD (SEGÚN PONDERACIÓN DE CONTROLES)	RIESGO RESIDUAL: IMPACTO (SEGÚN PONDERACIÓN DE CONTROLES)	VALORACIÓN DESPUÉS DE CONTROL (NIVEL DE RIESGO)		OPCIÓN DE MANEJO (ACCIONES)	REGISTROS	RESPONSABLE	FECHA DE TERMINACION.
Recurso Humano	R1	Indisponibilidad del Servicio de Mantenimiento de Equipos.	Alteración o eliminación de la información en el proceso	Perdida de la continuidad del negocio, servicios afectados para los usuarios internos y externos. Afectación a toda la Entidad	4	5	20	EVITAR EL RIESGO por medio de acciones de control preventivo que permita reducir la probabilidad de la ocurrencia del riesgo detectado.	Irregularidades encontradas en el proceso deben ser reportadas a control interno disciplinarioo a quien corresponda antes de generar una sanción o amonestación.	Preventivo	10	15	30	5	0	15	0	75	175	4	3	12	RIESGO ALTO	Reporte a Control Interno	Actas de Reunión	Responsable del proceso	2018-12-29
			Robo de información sensible en el proceso						Acceso a la información y a las funciones de los sistemas de las aplicaciones, se debe restringir su acceso.	Preventivo	10	15	0	5	0	15	0	45						Elaboración de reportes de acceso a los equipos	Verificar Roles y Responsabilidades		
			Demora en el envió de la Información al usuario						Procedimientos establecidos y documentados para detectar o corregir las fallas en el proceso rápidamente	Correctivo	10	15	0	5	0	15	0	45						Reporte de fallas	Documento		
			Pérdida de la información durante la recolección de datos en el proceso.						Desarrollo de campañas de concienciación en temas de seguridad de	Preventivo	10	0	0	0	0	0	0	10						Reuniones, campañas, Talleres	Actas de Reunión		
	R2	Falta de personal debidamente capacitado para la realización de las actividades del proceso.	El encargado del proceso no se encuentra disponible.	Fallas en procesos de seguridad de la información, perdida o robo de información de la entidad, Daños a los bienes o propiedad de la entidad	4	4	16	EVITAR EL RIESGO por medio de acciones de control preventivo que permita reducir la probabilidad de la ocurrencia del riesgo detectado.	Concientización del personal respecto a la seguridad de la información en procedimientos concernientes al mantenimiento preventivo y correctivo de equipos	Preventivo y Correctivo	10	0	0	0	0	0	0	10	190	4	2	8	RIESGO ALTO	Reuniones, campañas, Talleres y foros	Actas de Reunión	Responsable del proceso	2018-12-29
			Ausencia de transferencia de conocimiento y falta de capacitación tecnica						Establecer en el proceso mejores procesos de capacitación del personal. y/o contar con el equipo externo ideneo para la realizacion de esta actividad.	Preventivo	10	15	30	5	0	15	0	60						Capacitaciones	Actas, listado de asistencias, Informes		
			Inadecuada manipulación de los equipos por parte de personal ajeno al área encargada						Capacitaciones, procedimientos establecido para la manipulación de equipos de computo, previo acompañamiento por parte del responsable del proceso.	Preventivo	10	15	30	5	0	15	0	60						Reuniones, campañas, Talleres y foros	Actas de Reunión		
			No seguir el protocolo adecuado para el manejo y manipulación de equipos.						Capacitaciones, procedimientos establecido para la manipulación de equipos.	Preventivo	10	15	30	5	0	15	0	60						Reuniones, campañas, Talleres y foros	Actas, listado de asistencias,		
Servicios	R3	Interrupción completa en la continuidad del negocio (Daño en Data Center, Servicios Tecnológicos y pérdida de la Información	Eventos catastróficos: inundaciones, incendios, terremotos.	Interrupción completa de los servicios ofrecidos en la entidad	3	5	15	REDUCIR EL RIESGO por medio de acciones de control correctivas y preventivas que permita evitar la ocurrencia del riesgo	Centro de datos alterno en donde se espera reconstituir y reanudar a la operación normal de los procesos misionales de la entidad.	Preventivo	0	0	0	0	0	0	0	0	0			15	RIESGO EXTREMO	Elaborar el plan de continuidad de Negocio.	Documentos	Responsable de la seguridad de la Información	2018-12-29
Datos/Información	R4	Afectación de la integridad de los datos	Incumplimiento en las condiciones del servicio para los usuarios, funcionarios, colaboradores y clientes	Perdida de la información y posibles Ataques a la integridad de los datos.	4	4	16	EVITAR EL RIESGO por medio de acciones de control preventivo que permita reducir la probabilidad de la ocurrencia del riesgo detectado.	Aseguramiento, backup y respaldo de los archivos relevantes de la entidad.	Preventivo	10	0	0	5	0	0	0	15	125	4	2	8	RIESGO ALTO	Realizar un monitoreo al Aseguramiento	Análisis de los Datos y Reportes	Responsable del proceso	
			Pérdida o corrupción de los datos sistematizados de los diferentes procesos de la organización.						Copias de seguridad, para tener respaldos y evitar daños, redundancia cíclica. Inclusión en el plan de Backups de todos los servicios criticos de la entidad.	Preventivo	10	15	30	5	15	0	15	75						Copias de seguridad en servidores de alta Disponibilidad	Registro de Copias de Seguridad		
			Insuficiencia en el aseguramiento de la base de datos						Crear procesos de mantenimiento mensual de las BD y depuración de índices. Monitoreo de posibles intrusiones indebidas a las BD	Preventivo	10	15	0	0	0	0	0	25						Monitoreo de Bases de Datos	Registro de Monitoreo de Bases de Datos		2018-12-29
			Niveles de seguridad de la información inadecuados.						Fortalecimiento de la seguridad en perfiles, y acceso a aplicaciones	Preventivo	10	0	0	0	0	0	0	10						Documentar la seguridad en perfiles de Acceso	Documento		
	R5	Afectación de la disponibilidad del respaldo de la información en los procesos	Falla en el software del repositorio de Información Backup	Afectación a la disponibilidad de acceso al servicio o recurso de los diferentes procesos de la entidad	4	4	16	EVITAR EL RIESGO por medio de acciones de control preventivo que permita reducir la probabilidad de la ocurrencia del riesgo detectado.	Realización del Mantenimiento adecuado	Correctivo	10	0	0	5	0	0	0	15	25	4	4	16	RIESGO EXTREMO	Realizar el contrato de mantenimiento del software	Actas y Documentos	Responsable del proceso	
			Corrupción de las cintas en el momento de las copias y las restauración del Backups						Restauración de pruebas de información / Transporte, custodia y almacenamiento técnico para salvaguardar la información contenida en las cintas.	Correctivo	10	0	0	0	0	0	0	10						Realizar el contrato de transporte y custodia de cintas de Servidores / Verificar	Acta del procedimiento de salida de las cintas		
Software y/o Aplicaciones	R6	Funcionamiento inadecuado del aplicaciones de software que afectan losdiferentes procesos de la organización	Bloqueos a nivel de servicios de las aplicaciones	Mal funcionamiento del software, retraso en los procesos asociados a las aplicaciones de software de la entidad	4	3	12	REDUCIR EL RIESGO por medio de acciones de control correctivas y preventivas que permita evitar la ocurrencia del riesgo	Monitoreo preventivo diario para determinar anormalidades en los diferentes servicios de las aplicaciones misionales instaladas en los servidores.	Preventivo	10	15	30	5	15	0	15	75	150	4	1	4	RIESGO BAJO	Monitoreo de Logs	Reporte de Actividad	Responsable del proceso	2018-12-29
			Bloqueos a nivel de logs de las aplicaciones (congelamiento o intrusión)						Realizar monitoreo diario del espacio en disco para evitar que el tamaño de los logs desborde el espacio asignado.	Preventivo	10	15	30	5	15	0	15	75						monitoreo de Logs	Reporte de Actividad		
Equipos Informáticos (Hardware)	R7	Indisponibilidad de servidores, aires acondionados y equipos de computo	Obsolescencia Tecnológica	Perdida de la continuidad del negocio, servicios afectados para los usuarios internos y externos. Afectación a toda la Entidad	4	4	16	REDUCIR EL RIESGO por medio de acciones de control correctivas y preventivas que permita evitar la ocurrencia del riesgo	Se debe contar con el correspondiente plan de cambio y actualización de equipos para evitar rezagos tecnológicos no programados.	Preventivo	10	0	0	5	0	0	0	15	135	4	2	8	RIESGO ALTO	Elaboración de plan Actualización y cambio de piezas de hardware	Documento	Responsable del proceso	
			Falta de espacio por alto consumo de recursos						Monitoreo diario de los servidores, para verificar su estado y funcionamiento.	Preventivo	10	15	30	5	15	0	15	75						Reporte Mensual de análisis del monitoreo	Reporte de Actividad / Checklist		
			Puertos abiertos y servicios asociados que pueden causar la caída o falla de servidores						Monitoreo diario de los servidores, para verificar su estado y funcionamiento.	Preventivo	10	15	0	5	15	0	15	45						Reporte Mensual de análisis del monitoreo destinado para la	Reporte de Actividad / Checklist		
	R8	Funcionamiento inadecuado del almacenamiento	Saturación de capacidad de almacenamiento.	Perdida de informa ción.	3	4	12	EVITAR EL RIESGO por medio de acciones de control preventivo que permita reducir la probabilidad de la ocurrencia del riesgo detectado.	Realizar los correspondientes Backups para liberar espacio. Tareas programadas y monitoreadas	Preventivo	10	15	30	5	15	0	15	75	150	3	2	6	RIESGO MODERADO	Reporte Semanal de Backups de servidores.	Reporte de Actividad	Responsable del proceso	2018-12-29
			Reporte de alarmas en los arreglos de discos						Contactar al proveedor para que atienda el servicio en discos de servidores.	Preventivo	10	15	30	5	15	0	15	75						Reporte Semanal de la ocupación de Discos de Servidores.	Reporte de Actividad		
Redes de Comunicaciones	R9	Ausencia de integridad de la información en las comunicaciones para el desarrollo de los procesos	Ataques informáticos frente a la seguridad de la información.	Perdida, robo o mala utilización de la información.	4	5	20	REDUCIR EL RIESGO por medio de acciones de control correctivas y preventivas que permita evitar la ocurrencia del riesgo	Monitoreo preventivo para determinar anormalidades, fortaleciendo la seguridad activa de la red.	Preventivo	10	0	0	0	0	0	0	10	17			20	RIESGO EXTREMO	Reporte Diario del Trafico de la Red.	Logs, y Reporte de la Actividad	Responsable del proceso	

EQUIVALENCIAS	HERRAMIENTAS PARA EJERCER CONTROL	MANUALES, INSTRUCTIVOS O PROCEDIMIENTOS	EFECTIVIDAD DEL CONTROL	RESPONSABLES DEL CONTROL Y SEGUIMIENTO	EL CONTROL ES AUTOMATICO	EI CONTROL ES MANUAL	FRECUENCIA DE EJECUCIÓN DEL CONTROL Y SEGUIMIENTO	VALOR PXI (PROBABILIDAD X IMPACTO)
SI	(10 Puntos)	(15 Puntos)	(30 Puntos)	(5 Puntos)	(15 Puntos)	(15 Puntos	(15 Puntos)	
NO	(0 Puntos)	(0 Puntos)	(0 Puntos)	(0 Puntos)	(0 Puntos)	(0 Puntos)	(0 Puntos)	