MAPA DE RIESGOS DE ACTIVOS DE INFORMACIÓN

FECHA DE ACTUALIZACIÓN: 21 DE NOVIEMBRE DE 2024

FASE 3 - TRATAMIENTO DEL RIESGO

ACTIVOS DE LA ORGANIZACIÓN	RIESGOS DE CADA ACTIVO	NIVEL DE RIESGO	POSIBLE TRATAMIENTO
Inventario de equipos de cómputo	Riesgo de Pérdida: Los elementos del inventario pueden perderse o dañarse, lo que podría resultar en pérdidas financieras.	RIESGO MEDIO	El equipo de TI de la ACI Medellín cuenta con un inventario de los equipos de cómputo. Elabora un acta de entrega cuando es suministrado al funcionario. Se realiza semestralmente una inspección del estado de los equipos de computo.
UPS´s	Posibilidad de afectacion operacional debido a fallas por cortes no programados del fluido eléctrico	RIESGO ALTO	El equipo de TI de la ACI Medellín programa los mantenimiento preventivo regular en los UPS para garantizar su funcionamiento adecuado. Se monitorea el estado de los UPS para detectar problemas antes de que ocurran interrupciones.
Impresoras y Scaners	Falla técnica por acceso, consumible y/o atasco de papel.	RIESGO BAJO	El equipo de TI de la ACI Medellín realiza mantenimientos preventivos a las impresoras y coonfiguración a los diferentes equipos de los funcionarios.
Consola Antivirus	Acceso No Autorizado: Si la consola Antivirus no se protege adecuadamente, podría permitir el acceso no autorizado a la infraestructura de seguridad. Riesgos de Seguridad de la Consola: Vulnerabilidades en la propia consola podrían exponer la seguridad de la red interna.	RIESGO ALTO	El equipo de TI de la ACI Medellín protege la consola de antivirus con autenticación de múltiples factores. Monitorea la actividad en la consola para detectar actividades inusuales y mitigar riesgos de vulnerabilidad.
servidores virtuales	Interrupción de Servicio: Los servidores virtuales pueden experimentar interrupciones debido a fallas técnicas o ataques, lo que podría afectar la disponibilidad de servicios críticos.	RIESGO EXTREMO	El equipo de TI de la ACI Medellín implementa medidas de seguridad sólidas, como firewalls y detección de intrusiones, en los servidores virtuales. Mantiene actualizado el software del servidor y aplica parches de seguridad mensual. Realiza copias de seguridad mensuales.
Dispositivos de red	Acceso No Autorizado: Los dispositivos de red mal configurados pueden ser vulnerables a accesos no autorizados. Interrupciones de Red: Las fallas de los dispositivos de red pueden afectar la conectividad	RIESGO ALTO	El equipo de TI de la ACI Medellín configura contraseñas fuertes y cambia las credenciales predeterminadas en los dispositivos de red. Mantiene el firmware de los dispositivos actualizado y parcheado. Implementa monitoreo de seguridad de red para detectar actividades maliciosas.
Tenant de administración de Microsoft	Acceso No Autorizado: La falta de control de acceso adecuado en el tenant de administración de Microsoft puede exponer datos y configuraciones críticas. Problemas de Configuración: Errores de configuración pueden dar lugar a problemas de cumplimiento y seguridad.	RIESGO MEDIO	El equipo de TI de la ACI Medellín establece políticas de acceso y autenticación sólidas en el tenant de administración de Microsoft. Realiza auditorías regulares de seguridad y revisa la configuración para asegurarse de que cumple con las mejores prácticas.
Docuware	Vulnerabilidades en la Plataforma: Vulnerabilidades de seguridad en la plataforma DocuWare pueden exponer datos y documentos. Falta de Control de Acceso: La falta de control de acceso adecuado a los documentos almacenados en DocuWare puede ser un riesgo.	RIESGO ALTO	El equipo de TI de la ACI Medellín solicita al proveedor el acceso a la plataforma, utiliza cifrado para proteger los documentos almacenados en DocuWare. Realiza auditorías regulares al proveedor para asegurarse de que las políticas de seguridad se cumplan.
Dispositivos de control de acceso	Fallas Técnicas: Se puede experimentar fallas técnicas que afecten la seguridad y la protección del acceso a las instalaciones.	RIESGO BAJO	El equipo de TI de la ACI Medellín implementa medidas de seguridad física, como control de acceso a las instalaciones, para proteger los dispositivos de control de acceso. Actualiza el firmware y aplicar parches de seguridad en estos dispositivos.
CRM	Fugas de Datos del Cliente: La exposición de datos de clientes podría tener graves implicaciones legales y de reputación. Problemas de Privacidad: Las regulaciones de privacidad, como el RGPD, requieren la protección de los datos del cliente, y un CRM no configurado adecuadamente podría incumplir estas regulaciones. Inaccesibilidad de la información almacenada en el CRM	RIESGO ALTO	El equipo de TI de la ACI Medellín solicita acceso y autenticación sólidas al CRM para proteger los datos de los aliados, contactos, oportunidades de acuerdo a los roles establecidos para cada licencia. En caso de no continuidad del servicio se configuran copias y BK de informacion y de configuracion las cuales son almacenadas en la ruta https://acimedellinn.sharepoint.com/:f:/s/informatica/EsLBnBhdsPJHkPivURrxKTkBUqpD3HZsOwwaE-zdoWcJiA?e=ckjfrM en caso de presentarse fuga, se pueda restablecer el servicio. Monitorea las actividades del CRM para detectar comportamientos inusuales.
SharePoint	Acceso No Autorizado: Los permisos inadecuados o la configuración incorrecta de SharePoint podrían permitir el acceso no autorizado a documentos y datos confidenciales.	RIESGO ALTO	El equipo de TI de la ACI Medellín configura políticas de control de acceso y autenticación para proteger documentos y datos en SharePoint.
Carpetas Compartidas	Acceso No Autorizado: La falta de control de acceso adecuado a las carpetas compartidas puede exponer documentos y datos a personas no autorizadas. Pérdida de Datos: La eliminación accidental o la corrupción de datos en carpetas compartidas pueden tener consecuencias negativas.	RIESGO ALTO	El equipo de TI de la ACI Medellín establece control de acceso adecuado para garantizar que solo las personas autorizadas tengan acceso a las carpetas compartidas. Utiliza cifrado para proteger los datos almacenados en carpetas compartidas. Implementa políticas de seguridad que rigen el acceso y la retención de datos.