MATRIZ DE RIESGOS

								PROPIEDAD			VALORACION DEL ACTIVO									IDENTIFICACIÓN DE RIESGOS				PLAN DE TRATAMIENTO DE RIESGOS		
ID	DESCRIPCION DEL ACTIVO	TIPO DE PROCESO	PROCESO	SEDE	ACTIVO DE INFORMACIÓN	CATEGORIA DEL ACTIVO	UBICACIÓN (CONTENEDOR) DEL ACTIVO DE INFORMACIÓN	PROPIETARIO	CUSTODIO	CLASIFICACION DEL ACTIVO	C	I	D	VC	VI	VD	VF	CID	CLASIFICACIÓN DE LA INFORMACIÓN	VULNERABILIDADES	AMENAZAS	ESCENARIOS DE RIESGOS	DESCRIPCIÓN DEL RIESGO	ESTRATEGIA DE TRATAMIENTO DEL RIESGO	CONTROL PLAN DE ACCION	RESPONSABLE
RC1	BASE DE DATOS SQL MANAGER PARA LA APLICACIÓN SINCOW	MISIONAL	SUBDIRECCION ADMINISTRATIVA Y FINANCIERA	1 PISO 3	SERVIDOR DE BASE DE DATOS	EQUIPAMIENTO INFORMATICO	• Servidor de Aplicaciones	SUBDIRECCION ADMINISTRATIVA Y FINANCIERA	OFICINA DE INFORMACION Y COMUNICACIONES	SOFTWARE	A	A	A	4	4	4	4	A	RESERVADA	• Falta de lineamientos para el control de acceso físico. • Falta de un sistema para el control de acceso físico • Ausencia de sistemas de control ambiental que permitan controlar variables como temperatura y humedad	• Virus Informaticos • Acceso de personal no autorizado • Red cableada expuesta para el acceso no autorizado • Suplantacion de Identidad • Espionaje remoto • Manipulacion de Hardware	**Indisponibilidad de servicios esenciales.**	La indisponibilidad de servicios esenciales debido al acceso de personal no autorizado por la ausencia de lineamientos y de un sistema para el control de acceso físico que afectaría la disponibilidad, integridad y confidencialidad de la información.	Reducir el riesgo	• Definir y establecer una politica de acceso físico (Areas seguras). • Implementar un sistema biometrico que permita solo el acceso a personal autorizado.	Oficina de Información y Comunicaciones
RC2	BASE DE DATOS DE BUSES Y TAXIS INTERMUNICIPALES Y URBANOS	MISIONAL	SUBDIRECCION TECNICA DE TRANSPORTE	1 PISO 1	SERVIDOR DE BASE DE DATOS	EQUIPAMIENTO INFORMATICO	• Servidor de Aplicaciones	SUBDIRECTOR DE TRANSPORTE	OFICINA DE INFORMACION Y COMUNICACIONES	SOFTWARE	A	A	MA	4	4	5	4	A	RESERVADA	• Falta de lineamientos para el control de acceso físico. • Falta de un sistema para el control de acceso físico • Ausencia de sistemas de control ambiental que permitan controlar variables como temperatura y humedad	• Virus Informaticos • Acceso de personal no autorizado • Red cableada expuesta para el acceso no autorizado • Suplantacion de Identidad • Espionaje remoto • Manipulacion de Hardware	**Indisponibilidad de servicios esenciales.**	La indisponibilidad de servicios esenciales debido al acceso de personal no autorizado por la ausencia de lineamientos y de un sistema para el control de acceso físico que afectaría la disponibilidad, integridad y confidencialidad de la información.	Reducir el riesgo	• Definir y establecer una politica de acceso físico (Areas seguras). • Implementar un sistema biometrico que permita solo el acceso a personal autorizado.	Oficina de Información y Comunicaciones
RC3	APLICATIVO PARA LA GESTION DOCUMENTAL	MISIONAL	SUBDIRECCION ADMINISTRATIVA Y FINANCIERA	1 PISO 1 Y 3	SERVIDOR DE APLICACIONES	SOFTWARE - APLICACIONES INFORMATICAS	• Servidor de Aplicaciones	SUBDIRECCION ADMINISTRATIVA Y FINANCIERA	OFICINA DE INFORMACION Y COMUNICACIONES	SOFTWARE	A	A	MA	4	4	5	4	A	INTERNA	• Falta de lineamientos para el control de acceso físico. • Falta de un sistema para el control de acceso físico • Ausencia de configuraciones de seguridad en el aplicativo que permita solicitar el cambio de la contraseña con el aprovisionamiento del servicio de un usuario nuevo. • El software no cuenta con lineamientos de seguridad que	• Virus Informaticos • Acceso de personal no autorizado • Red cableada expuesta para el acceso no autorizado • Suplantacion de Identidad • Espionaje remoto • Manipulacion de Hardware	**Indisponibilidad de servicios esenciales.**	La indisponibilidad de servicios esenciales debido al acceso de personal no autorizado por la ausencia de lineamientos y de un sistema para el control de acceso físico que afectaría la disponibilidad, integridad y confidencialidad de la información.	Reducir el riesgo	• Definir y establecer una politica de acceso físico (Areas seguras). • Implementar un sistema biometrico que permita solo el acceso a personal autorizado.	Oficina de Información y Comunicaciones
RC4	SISTEMA OPERATIVO PARA LA GESTION DE USUARIOS EN EL DOMINIO	MISIONAL	SUBDIRECCION ADMINISTRATIVA Y FINANCIERA	1 PISO 3	SERVIDOR DE APLICACIONES	SOFTWARE - APLICACIONES INFORMATICAS	• Servidor de Aplicaciones	OFICINA DE INFORMACION Y COMUNICACIONES	OFICINA DE INFORMACION Y COMUNICACIONES	SOFTWARE	A	A	A	4	4	4	4	A	SENSIBLE	• Falta de lineamientos para el control de acceso físico. • Falta de un sistema para el control de acceso físico • Ausencia de sistemas de control ambiental que permitan controlar variables como temperatura y humedad	• Virus Informaticos • Acceso de personal no autorizado • Red cableada expuesta para el acceso no autorizado • Suplantacion de Identidad • Espionaje remoto • Manipulacion de Hardware	**Indisponibilidad de servicios esenciales.**	La indisponibilidad de servicios esenciales debido al acceso de personal no autorizado por la ausencia de lineamientos y de un sistema para el control de acceso físico que afectaría la disponibilidad de la información.	Reducir el riesgo	• Definir y establecer una politica de acceso físico (Areas seguras). • Implementar un sistema biometrico que permita solo el acceso a personal autorizado.	Oficina de Información y Comunicaciones
RC5	SOFTWARE ORIENTADO AL CONTROL Y PROTECCION DE LA RED DE CODIGO MALICIOSO Y ACCESOS NO AUTORIZADOS A LOS USUARIOS	APOYO	SUBDIRECCION ADMINISTRATIVA Y FINANCIERA	1 PISO 3	CONSOLA ATIVIRUS	SOFTWARE - APLICACIONES INFORMATICAS	• Equipos de cómputo (Portátiles y de escritorio) • Servidores	OFICINA DE INFORMACION Y COMUNICACIONES	OFICINA DE INFORMACION Y COMUNICACIONES	SOFTWARE	A	A	A	4	4	4	4	A	INTERNA	• Falta de cumplimiento de las politicas de seguridad por parte de funcionarios correspondiente a. • Falta de un sistema para el control de acceso físico	• Virus Informaticos • Acceso de personal no autorizado • Red cableada expuesta para el acceso no autorizado • Suplantacion de Identidad • Espionaje remoto	**Indisponibilidad de servicios esenciales.**	La indisponibilidad de servicios esenciales debido al acceso de personal no autorizado por la ausencia de lineamientos y de un sistema para el control de acceso físico que afectaría la disponibilidad de la información.	Reducir el riesgo	• Definir y establecer una politica de acceso físico (Areas seguras). • Implementar un sistema biometrico que permita solo el acceso a personal autorizado.	Oficina de Información y Comunicaciones
RC6	HERRAMIENTA PARA LA GESTION DE CALIDAD	APOYO	CONTROL INTERNO	1 PISO 3	SISTEMA PARA LA GESTION DE CALIDAD	DATOS E INFORMACION	• Servidor de Aplicaciones • Computador del Asesor de Control Interno	JEFE DE CONTROL INTERNO	OFICINA DE INFORMACION Y COMUNICACIONES	PROCEDIMENTAL Y ESTRUCTURAL	M	A	M	3	4	3	3	M	INTERNA	• Falta de acceso seguro al archivo fisico de control interno. • Falta de politica interna para las copias de seguridad de informacion.	• Acceso de personal no autorizado • Suplantacion de Identidad • Espionaje remoto • Manipulacion de software	**Pérdida de información**	La perdida de informacion causada por daños fisicos de dispositivos de almacenamiento o ataques informaticos, afectaría la disponibilidad e integridad de la información.	Reducir el riesgo	• Establecer la implementacion de un nuevo sistema de gestion mas robusto. • Implementar politicas de seguridad de mayor alcance.	Oficina de Control Interno
RC7	CONSOLA DE ADMINISTRACION ONLINE PARA LA GESTION DEL CORREO CORPORATIVO	APOYO	SUBDIRECCION ADMINISTRATIVA Y FINANCIERA	1 PISO 3	CUENTAS DE CORREO CORPORATIVAS	SOFTWARE - APLICACIONES INFORMATICAS	• Equipos de cómputo (Portátiles y de escritorio) • Servidores	OFICINA DE INFORMACION Y COMUNICACIONES	OFICINA DE INFORMACION Y COMUNICACIONES	SOFTWARE	A	A	B	4	4	2	3	M	INTERNA	• Falta de lineamientos para el control de acceso físico. • Falta de un sistema para el control de acceso físico	• Virus Informaticos • Acceso de personal no autorizado • Red cableada expuesta para el acceso no autorizado • Suplantacion de Identidad • Espionaje remoto	**Indisponibilidad de servicios esenciales.**	La indisponibilidad de servicios esenciales debido al acceso de personal no autorizado por la ausencia de lineamientos y de un sistema para el control de acceso físico que afectaría la disponibilidad de la información.	Reducir el riesgo	• Definir y establecer una politica de acceso físico (Areas seguras). • Implementar un sistema biometrico que permita solo el acceso a personal autorizado.	Oficina de Información y Comunicaciones
RC8	DISCOS DUROS EXTERNOS PARA LAS COPIAS DE SEGURIDAD	APOYO	SUBDIRECCION ADMINISTRATIVA Y FINANCIERA	1 PISO 3	MEDIOS EXTRAIBLES	DATOS E INFORMACION	• Equipos de cómputo (Portátiles y de escritorio) • Servidores	OFICINA DE INFORMACION Y COMUNICACIONES	OFICINA DE INFORMACION Y COMUNICACIONES	HARDWARE	M	A	B	3	4	2	3	M	INTERNA	• No se establece ningún proceso de cifrado de información en unidades de almacenamiento externas como USB, discos duros (Internos y/o externos). • Ausencia de niveles de protección física sobre los dispositivos de almacenamiento externo. • No se realizan procesos de borrado seguro de la	• Pérdida y/o fuga de información confidencial de la organización por hurto de unidades de almacenamiento de información externos.	**Pérdida de información**	La perdida de informacion causada por daños fisicos de dispositivos de almacenamiento o ataques informaticos, afectaría la disponibilidad e integridad de la información.	Reducir el riesgo	• Clasificar la información de la organización, definiendo si es pública, privada o confidencial. • Implementar mecanismos de cifrado de información en unidades de almacenamiento (Discos duros, USB, portátiles y dispositivos móviles). • Adquirir el servicio de almacenamiento de informacion	Oficina de Información y Comunicaciones - Subdireccion Administrativa y Financiera
RC9	ARCHIVO FISICO GENERAL DE LA ENTIDAD, POSEE TODA LA INFORMACION INSTITUCIONAL	MISIONAL	SUBDIRECCION ADMINISTRATIVA Y FINANCIERA	1 PISO 1	ARCHIVO FISICO	DOCUMENTOS E INFORMACIÓN	• Area de Gestión Documental, Contiene información foleada de toda la instiutción.	SUBDIRECCION ADMINISTRATIVA Y FINANCIERA	LIDER DEL PROCESO DE GESTION DOCUMENTAL	SITIO	A	A	B	4	4	2	3	M	INTERNA	• Falta de un sistema para el control de acceso físico. Se evidencia que no existe el control de acceso a usuarios. No existe un manejo de llaves o algun tipo de seguridad para acceder • Ausencia de sistemas de control de humedad que permitan controlar variables de humedad.	• Hurto o pérdida de información causada por parte de un empleado o externo • Afectación temporal de la disponibilidad de la información • Fuego – Posibilidad de que un incendio destruya los recursos y activos de la	**Pérdida de información**	La perdida de información causada por hurto o daños fisicos de documentos afectaria la disponibilidad, integridad y confidencialidad de la información.	Reducir el riesgo	• Definir y establecer una politica de acceso físico (Areas seguras). • Implementar un sistema biometrico que permita solo el acceso a personal autorizado. • Diseñar y/o actualizar la política de seguridad de la información de la organización para los archivos fisicos.	Lider del Proceso de Gestión Documental - Lider de Proceso de Subdireccion Administrativa y Financiera
RC10	ARCHIVO FISICO QUE CONTIENE DOCUMENTOS, ACTAS Y RESOLUCIONES	APOYO	SECRETARIA GENERAL	1 PISO 3	ARCHIVO FISICO	DOCUMENTOS E INFORMACIÓN	• Archivo Fisico, folder y cajas ubicado bajo llave con acceso restringido y autorizado por el lider del proceso	SECRETARIO GENERAL	SECRETARIO GENERAL	SITIO	A	A	MB	4	4	1	3	M	INTERNA	• Ausencia de sistemas de control de humedad que permitan controlar variables de humedad. • Ausencia de camaras internas para el control de entreda salida	• Hurto o pérdida de información causada por parte de un empleado descontento de la entidad. • Afectación temporal de la disponibilidad e integridad de la información • Presentación de condiciones inadecuadas	**Pérdida de información**	La perdida de información causada por hurto o daños fisicos de documentos afectaria la disponibilidad, integridad y confidencialidad de la información.	Reducir el riesgo	• Definir y establecer una politica de acceso físico (Areas seguras). • Diseñar y/o actualizar la política de seguridad de la información de la organización para los archivos fisicos. • Implemetar mecanismos para el control de humedad.	Secretaria General - Subdireccion Administrativa y Financiera
RC11	ARCHIVO FISICO QUE CONTIENE DOCUMENTOS, ACTAS Y RESOLUCIONES	APOYO	TALENTO HUMANO	1 PISO 3	ARCHIVO FISICO	DOCUMENTOS E INFORMACIÓN	• Archivo Fisico, folder y cajas ubicado bajo llave con acceso restringido y autorizado por el lider del proceso	LIDER PROCESO DE TALENTO HUMANO	LIDER PROCESO DE TALENTO HUMANO	PROCEDIMENTAL Y ESTRUCTURAL	A	A	MB	4	4	1	3	M	INTERNA	• Ausencia de sistemas de control de humedad que permitan controlar variables de humedad. • Ausencia de camaras internas para el control de entreda salida	• Hurto o pérdida de información causada por parte de un empleado descontento de la entidad. • Afectación temporal de la disponibilidad e integridad de la información • Presentación de condiciones inadecuadas	**Pérdida de información**	La perdida de información causada por hurto o daños fisicos de documentos afectaria la disponibilidad, integridad y confidencialidad de la información.	Reducir el riesgo	• Definir y establecer una politica de acceso físico (Areas seguras). • Diseñar y/o actualizar la política de seguridad de la información de la organización para los archivos fisicos. • Implemetar mecanismos para el control de humedad.	Lider del Proceso de Talento Humano - Subdireccion Administrativa y Financiera
RC12	ARCHIVO FISICO QUE CONTIENE DOCUMENTOS, ACTAS Y RESOLUCIONES	APOYO	SUBDIRECCION DE PLANEACION	1 PISO 3	ARCHIVO FISICO	DOCUMENTOS E INFORMACIÓN	• Archivo Fisico, folder y cajas ubicado bajo llave con acceso restringido y autorizado por el lider del proceso	SUBDIRECTOR DE PLANEACION	SUBDIRECTOR DE PLANEACION	PROCEDIMENTAL Y ESTRUCTURAL	A	A	MB	4	4	1	3	M	INTERNA	• Ausencia de sistemas de control de humedad que permitan controlar variables de humedad. • Ausencia de camaras internas para el control de entreda salida	• Hurto o pérdida de información causada por parte de un empleado descontento de la entidad. • Afectación temporal de la disponibilidad e integridad de la información • Presentación de condiciones inadecuadas	**Pérdida de información**	La perdida de información causada por hurto o daños fisicos de documentos afectaria la disponibilidad, integridad y confidencialidad de la información.	Reducir el riesgo	• Definir y establecer una politica de acceso físico (Areas seguras). • Diseñar y/o actualizar la política de seguridad de la información de la organización para los archivos fisicos. • Implemetar mecanismos para el control de humedad.	Subdireccion de Planeación
RC13	ARCHIVO FISICO QUE CONTIENE DOCUMENTOS, ACTAS Y RESOLUCIONES	APOYO	SUBDIRECCION ADMINISTRATIVA Y FINANCIERA	1 PISO 3	ARCHIVO FISICO	DOCUMENTOS E INFORMACIÓN	• Archivo Fisico, folder y cajas ubicado bajo llave con acceso restringido y autorizado por el lider del proceso, este espacio es compartido para las areas de Tesoreria, Presupuesto y Contabilidad	SUBDIRECTOR ADMINISTRATIVO Y FINANCIERO	SUBDIRECTOR ADMINISTRATIVO Y FINANCIERO	PROCEDIMENTAL Y ESTRUCTURAL	A	A	MB	4	4	1	3	M	INTERNA	• Ausencia de sistemas de control de humedad que permitan controlar variables de humedad. • Ausencia de camaras internas para el control de entreda salida	• Hurto o pérdida de información causada por parte de un empleado descontento de la entidad. • Afectación temporal de la disponibilidad e integridad de la información • Presentación de condiciones inadecuadas de temperatura y humedad que generan daños sobre la infraestructura física.	**Pérdida de información**	La perdida de información causada por hurto o daños fisicos de documentos afectaria la disponibilidad, integridad y confidencialidad de la información.	Reducir el riesgo	• Definir y establecer una politica de acceso físico (Areas seguras). • Diseñar y/o actualizar la política de seguridad de la información de la organización para los archivos fisicos. • Implemetar mecanismos para el control de humedad.	Lider del Proceso de Tesoreria, Contabilidad y Presupuesto - Subdireccion Administrativa y Financiera
RC14	ARCHIVADOR METALICO	APOYO	TESORERIA	1 PISO 3	ARCHIVO FISICO	DOCUMENTOS E INFORMACIÓN	• Archivador metalico ubicado en el area finaniera, contiene información institucional y comprobantes	LIDER DEL PROCESO DE TESORERIA	LIDER DEL PROCESO DE TESORERIA	SITIO	A	A	MB	4	4	1	3	M	INTERNA	• Falta de sistemas de control para acceso, el archivador posee llave pero no existe control de uso • Falta de politica para el acceso fisico	• Hurto o pérdida de información causada por parte de un empleado descontento de la entidad. • Afectación temporal de la disponibilidad e integridad de la información • Presentación de condiciones inadecuadas de temperatura y humedad que generan daños sobre la infraestructura física.	**Pérdida de información**	La perdida de información causada por hurto o daños fisicos de documentos afectaria la disponibilidad, integridad y confidencialidad de la información.	Reducir el riesgo	• Definir y establecer una politica de acceso físico. • Trasladar la informacion a areas seguras para mayor control de la seguridad	Lider del Proceso de Tesoreria
RC15	ARCHIVADOR METALICO	APOYO	CONTABILIDAD	1 PISO 3	ARCHIVO FISICO	DOCUMENTOS E INFORMACIÓN	• Archivador metalico ubicado en el area finaniera, contiene información institucional	LIDER DEL PROCESO DE CONTABILIDAD	LIDER DEL PROCESO DE CONTABILIDAD	SITIO	A	A	MB	4	4	1	3	M	INTERNA	• Falta de sistemas de control para acceso, el archivador posee llave pero no existe control de uso • Falta de politica para el acceso fisico	• Hurto o pérdida de información causada por parte de un empleado descontento de la entidad. • Afectación temporal de la disponibilidad e integridad de la información • Presentación de condiciones inadecuadas de temperatura y humedad que generan daños sobre la infraestructura física.	**Pérdida de información**	La perdida de información causada por hurto o daños fisicos de documentos afectaria la disponibilidad, integridad y confidencialidad de la información.	Reducir el riesgo	• Definir y establecer una politica de acceso físico. • Trasladar la informacion a areas seguras para mayor control de la seguridad	Lider del Proceso de Contabilidad
RC16	ARCHIVADOR METALICO	MISIONAL	DIRECCION GENERAL	1 PISO 3	ARCHIVO FISICO	DOCUMENTOS E INFORMACIÓN	• Archivador metalico ubicado en el area de la asistente de dirección.	DIRECTOR	SECRETARIA	SITIO	A	A	M	4	4	3	3	M	INTERNA	• Falta de sistemas de control para acceso, el archivador posee llave generica. • Falta de politica para el acceso fisico	• Hurto o pérdida de información causada por parte de un empleado descontento de la entidad. • Afectación temporal de la disponibilidad e integridad de la información • Presentación de condiciones inadecuadas de temperatura y humedad que generan daños sobre la infraestructura física.	**Pérdida de información**	La perdida de información causada por hurto o daños fisicos de documentos afectaria la disponibilidad, integridad y confidencialidad de la información.	Reducir el riesgo	• Definir y establecer una politica de acceso físico. • Estableser mecanismo mas robustos de seguridad fisica como llaves electronicas. • Trasladar la informacion a areas seguras para mayor control de la seguridad	Dirección General
RC17	ARCHIVADOR METALICO	APOYO	INFORMACION Y COMUNICACIONES	1 PISO 3	ARCHIVO FISICO	DOCUMENTOS E INFORMACIÓN	• Archivador metalico ubicado en el area general	LIDER PROCESO DE COMUNICACIONES	LIDER PROCESO DE COMUNICACIONES	SITIO	A	A	M	4	4	3	3	M	INTERNA	• Falta de sistemas de control para acceso, el archivador posee llave generica. • Falta de politica para el acceso fisico	• Hurto o pérdida de información causada por parte de un empleado descontento de la entidad. • Afectación temporal de la disponibilidad e integridad de la información • Presentación de condiciones inadecuadas de temperatura y humedad que generan daños sobre la infraestructura física.	**Pérdida de información**	La perdida de información causada por hurto o daños fisicos de documentos afectaria la disponibilidad, integridad y confidencialidad de la información.	Reducir el riesgo	• Definir y establecer una politica de acceso físico. • Estableser mecanismo mas robustos de seguridad fisica como llaves electronicas. • Trasladar la informacion a areas seguras para mayor control de la seguridad	Lider del proceso de Comunicaciones
RC18	ESTACIONES DE TRABAJO Y PORTATILES ASIGNADOS A LOS FUNCIONARIOS Y ASESORES	APOYO	INFORMACION Y COMUNICACIONES	1 PISO 3	ESTACIONES DE TRABAJO Y PORTATILES	EQUIPAMIENTO INFORMATICO	• Lugar de trabajo asignado en los pisos 1 y piso 3	INFORMACION Y COMUNICACIONES	FUNCIONARIO ASIGNADO	SITIO	A	A	M	4	4	3	3	M	INTERNA	• Falta de control por parte de los funcionarios o asesores en cuanto al uso de las claves de acceso	• Hurto o pérdida de información. • Afectación temporal de la disponibilidad e integridad de la información	**Pérdida de información**	La perdida de información causada por hurto o saboteos de documentos afectaria la disponibilidad, integridad y confidencialidad de la información.	Reducir el riesgo	• Capacitar a los funcionarios respecto al uso correcto de claves y su importancia para protejer los activos de información	Funcionario o Asesor asignado
RC19	RED LAN DE AREA LOCAL INSTITUCIONAL	APOYO	INFORMACION Y COMUNICACIONES	1 PISO 3	RED DE AREA LOCAL	REDES DE COMUNICACIONES	• Instalacion fisica institucional en los pisos 1 y piso 3	INFORMACION Y COMUNICACIONES	INFORMACION Y COMUNICACIONES	SITIO	A	A	A	4	4	4	4	A	INTERNA	• Deficiencias en las configuraciones de seguridad de la red inalámbrica, empleando un cifrado débil. • Dispositivos de red (Router) obsoletos. • inestabilidad de servicio WIFI	• Acceso remoto no autorizado • Indisponibilidad del servicio de la red inalámbrica debido a ataques de denegación de servicios (DoS).	**Pérdida de información**	La perdida de información causada por hurto o daños fisicos de documentos afectaria la disponibilidad, integridad y confidencialidad de la información.	Reducir el riesgo	• Indisponibilidad de los servicios que se brindan a través de la red ocasionando tiempos no productivos del equipo de desarrollo de la organización.	Dirección General