CODIGO
RG01
RG02
RG03
RG04
RG05
RG06
RG07
RG07
RG08
RG09
RG10
RG11
RG12
RG13
RG14

CODIGO
RC01
RC02
RC03
RC04
RC05
RC06
RC07
RC08
RC09
RC10
RC11
RC12
RC13
RC14
RC15
RC16
RC17
RC18

RC19
RC20
RC21
RC22
RC23
RC24
RC25
RC26

CODIGO
RA01
RA02
RA03
RA04
RA05
RA06
RA07

CODIGO
RD01
RD02
RD03
RD04
RD05
RD06
RD07
RD08
RD09
RD10
RD11
RD12
RD13
RD14
RD15
RD16
RD17
RD18
RD19
RD20
RD21
RD22
RD23
RD24
RD25
RD26

RD27
RD28
RD29
RD30
RD31
RD32
RD33
RD34
RD35
RD36
CODIGO
RP01
RP02
RP03
RP04
RP05
RP06
RP07
RP08
RP09
RP10
CODIGO
RI01
RI02
RI03
RI04
RI05
RI06
RI07
RI08
RI09
CODIGO
RS01
RS02
RS03
RS04
RS05
RS05
RS07
RS08
RS09
RS10
RS11

RS12
RS13
RS14
RS15

El presente documento incluye una serie de riesgos básicos que pueden presentarse en la implementación y su objeti
referencia a la hora de completar la información en las tablas de los procesos. No es una lista exhaustiva de riesgos, c
que considere necesarios e inclusive puede no aplicar aquellos riesgos que considera no le aplican.

PORTAFOLIO DE RIESGOS NORMATIVA TECNOLOGIAS DE LA INFORMACION
RIESGO EN LA GESTION DE LA INFORMACION
Abuso de derechos por parte de los usuarios del sistema
Acceso no autorizado a aplicaciones por parte de los usuarios
Conformación inadecuada de contraseñas (insegura, débiles)
Uso compartido de contraseñas por parte de los usuarios
Robo o perdida de información por controles inadeacuados
Capacitación inadecuada a los usuarios del sistema en la forma de administrar los recursoa asignados
Confidencialidad de la información comprometida
Privacidad de la información comprometida
Problemas en el acceso a las aplicaciones
Integridad de la Información comprometida por usuarios internos
Integridad de la Información comprometida por accesos externos no autorizados
No hay disponibilidad de la información
Clasificación inadecuada de la información
Etiquetado onadecuado de la in formación
Robo o perdida de información por ataques de Hackers, Malware
RIESGOS EN LA GESTION DE LA CONTINUIDAD
Mala identificación de los respaldos de información
Respaldos de información no verificados
Respaldos de información almacenados en forma incorrecta
Inadecuado traslado y custodia de los respaldos
Técnicas de recuperación/restauración de los archivos no estandarizada
Errores en el respaldo y recuperación de los datos.
Interrupción del servicio por falta de capacidad de almacenamiento o por fallas en los dispositivos de almacer
Plan de continuidad o contingencia no documentado
Plan de continuidad o contingencia incompleto
Plan de continuidad o contingencia no probado
Plan de continuidad o contingencia no aprobado por las altas autoridades
Plan de continuidad o contingencia desactualizado
Personal interno poco preparado para enfrentar una contingencia
No se cuenta con suficiente personal para enfrentar una contingencia
Plan de continuidad o contingencia no comunicado a las partes interesadas
Robo o pérdida de medios de almacenamiento
Desastres naturales (terremotos, inundaciones, tornados, huracanes, etc.)
Incendio

Epidemia
Electromanetismo
Técnicas de recuperación/restauración de los archivos no estandarizada
Desorden civil
Acciones emprendidas por empleados inescrupulosos que pueden causar daños tanto a las instalaciones
Interrupciones prolongadas de los servicios básicos como la electricidad, el agua potable y las comunicacione
Actos criminales, como vandalismo, terrorismo, etc.
Robo o pérdida de medios de almacenamiento
RIESGOS EN LA GESTION DE LAS COMUNICACIONES
Fallas en la infraestructura tecnológica de los proveedores externos (ICE. RACSA, CNFL) que soporta la pre
Fallas en las comunicaciones debido problemas internos
Fallas por eventos que afecten las lineas de transmision internas o externas
Falta de disponibilidad en las lineas de comunicaciones
Fallas producidas por errores o problemas en la transmisión
Errores en la configuración de equipos de comunicaciones
Monitoreo inadecuado de las comunicaciones
RIESGOS EN CENTROS DE DATOS
Falta de disponibilidad del personal técnico (SO, base de datos, comunicaciones, etc.)
No existe de un plan formal, actulalizado y comunicado formalmente para la recuperación de las aplicaciones
Fallas eléctricas en el centro de cómputo
Daños que se presenten en los equipos por vandalismo, uso inadecuado o fallas en la administración
Datos se replican en forma incorrecta
Fallas en el equipo de aire acondicionado, UPS o planta eléctrica
Controles inadecuados para el monitoreo, seguimiento y protocolos formales para atención y escalamiento de
Aplicaciones anticuados que no soportan la carga de trabajo, el volumen, las funcionalidades
Inadecuado mantenimiento de los sistemas
Reprocesos en las pruebas y atrasos en la implementación por no contar con una infraestructura para la realiza
Dependencia de los proveedores para el suministro de servicios, repuestos o de mantenimientos a los equipos
Utilización incorrecta de los equipos de cómputo
Mal funcionamiento de una base de datos
Daño en una base de datos o archivos críticos
Problemas de acceso a una base de datos
Administración inadecuada de procesos de actualización
Falta de capacitación o capacitación iadecuada de los encaragados de los procesos de actualización
Falta de procedimientos o procedimientos inadecuados para la ejecución de tareas críticas
Controles deficientes en ambientes de pruebas
Controles deficientes en ambientes de producción
Falla en un servidor o varios a la vez
Pérdidas o suspensión temporal del servicio por una incorrecta configuración de parámetros en los sistemas
Errores en la configuración de equipos (servidores)
Mal diseño de las aplicaciones generando problemas de funcionamiento
Problemas en la distribución del cableado eléctrico o de comunicaciones
Insuficiente personal capacitado para realizar las tareas de operación, monitoreo y soporte de los servicios en

Afectación en la gestión ylos programas de trabajo porque no se realizron las pruebas de aceptación dentro
Inundación por daño de tuberías internas del edificio
Fallas producidas por errores de programación que afectan la calidad del servicio
Afectación del servicio por generación de incidentes y problemas asociados a una mala implementación de ca
Afectación del servicio por no tramitar oportunamente un cambio requerido urgente
Reprocesos en las pruebas y atrasos en la implementación por integración de aplicaciones incompletas o erró
Pérdida de información producidas por fallas en los controles de seguridad
Pérdida de información por la inadecuada utilización de los equipos de cómputo
No contar con las condiciones ambientales recomendadas por el fabricante para la operación adecuada de los
Pérdida de información por la inadecuada utilización de los sistemas en utilización en la Institución
RIESGOS EN LA GESTION DE PROVEEDORES
Incumplimiento de contratos por parte del proveedor
Incumplimiento de contratos por parte de la Institución
Deficiencias en los servicios de los proveedores
No contar con proveedores que estén preparados para ayudar a enfrentar una contingencia de tipo tecnológic
Alta dependencia de proveedores claves a nivel de tecnología para proporcionar los servicios
Contratos obsolectos
Fallas en la gestión de licenciamientos
Fallas en el control de vencimiento de los contratos
Iinexistencia de contratos
Contratos no alineados a niveles de servicio (SLA)
RIESGOS DE CUMPLIMIENTO
Incumplimiento por entrega de información incompleta a entes reguladores
Incumplimiento de la legislación vigente
Incumplimiento de normativas externas
Incumplimiento en las fechas de entrega de la información a entes reguladores
No contar con el apoyo de las altas autoridades
Insuficientes recursos (humanos, equipos, espacio físico, etc.) para trabajar en la implementación
No contar con una cultura de riesgos en la institución
Los responsables de TI no cuentan con el suficiente apoyo de las altas autoridades para realizar su gestión
No se cuenta con políticas institucionales para la gestión de TI
RIESGOS EN SEGURIDAD DE LA INFORMACION
Incumplimiento de políticas de seguridad
Falta de capacitación y concientizacion en seguridad de la información
Políticas de seguridad no documentadas o estan desactualizadas
Normativas de seguridad no documentadas o estan desactualizadas
Controles de seguridad no documentadas o estan desactualizadas
Procedimientos de seguridad no documentadas o estan desactualizadas
Procesos de seguridad no documentados o estan desactualizadas
Ataques de denegación de servicios
No se actualiza en forma adecuada la plataforma tecnológica que atiende los servicios de Internet
Plataforma de seguridad mal atendida, monitoreo inadecuado de incidentes de seguridad
Capacitación inadecuada en ingeniería social

Perdida de equipos de cómputo (principalmente portátiles) sin la debida protección, con la consiguiente perdi
Perfiles de acceso no definidos o mal congigurados
Red interna puede ser vulnerada por parte de cibercriminales
Gestión inadecuada en el parchado de aplicaciones o equipos

vo es que las Instituciones cuenten con una

stación de servicios, afectando la disponibilidad