ANEXOS

Anexo 1:
Modelamiento BPM de los principales procesos de una Central de Riesgo privada.

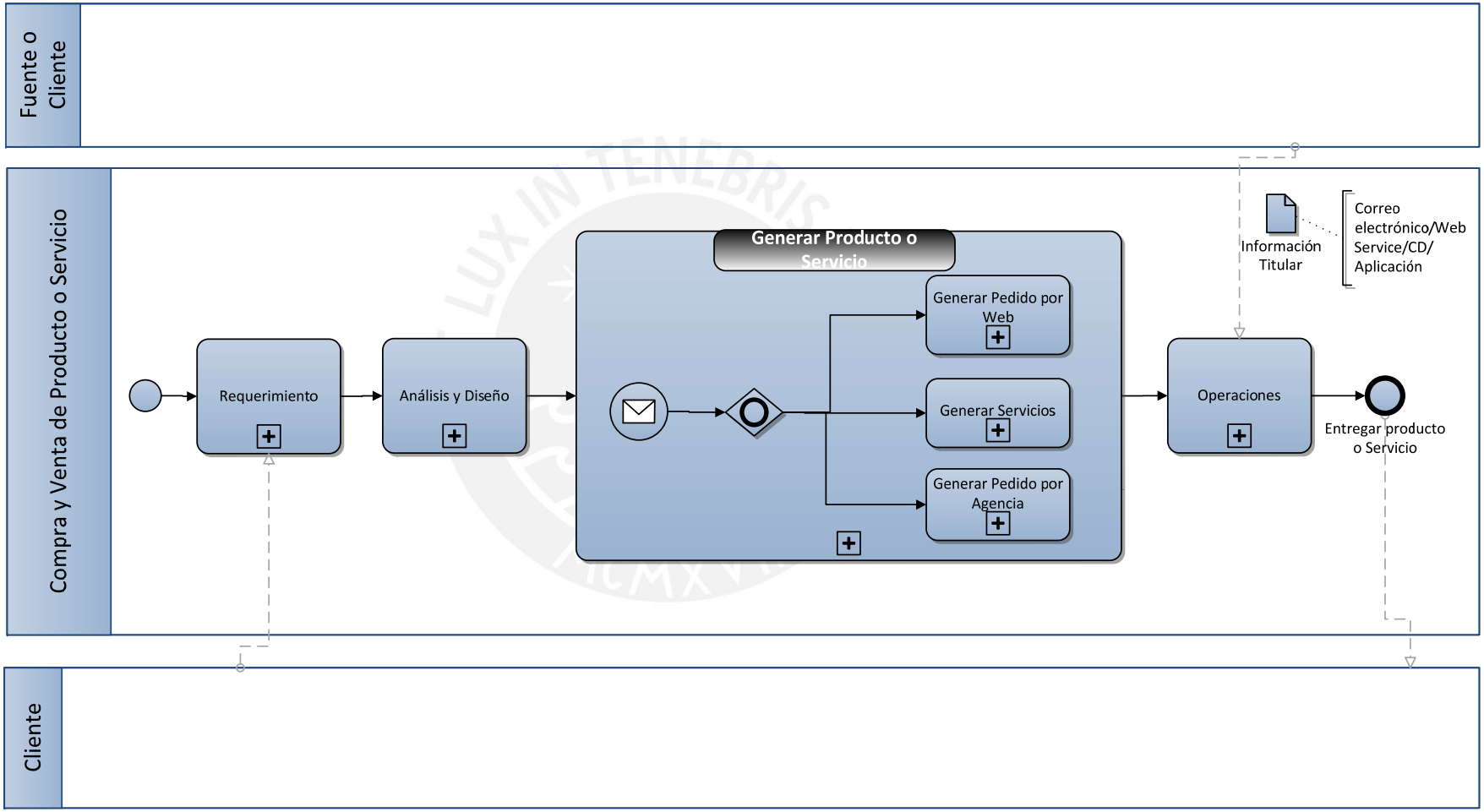
Anexo 2:
Valoración de los activos.

Anexo 3:
Matriz de Riesgos de los Procesos
Tratamiento de Riesgos
Mapeo Controles ISO 27001 con COBIT 5

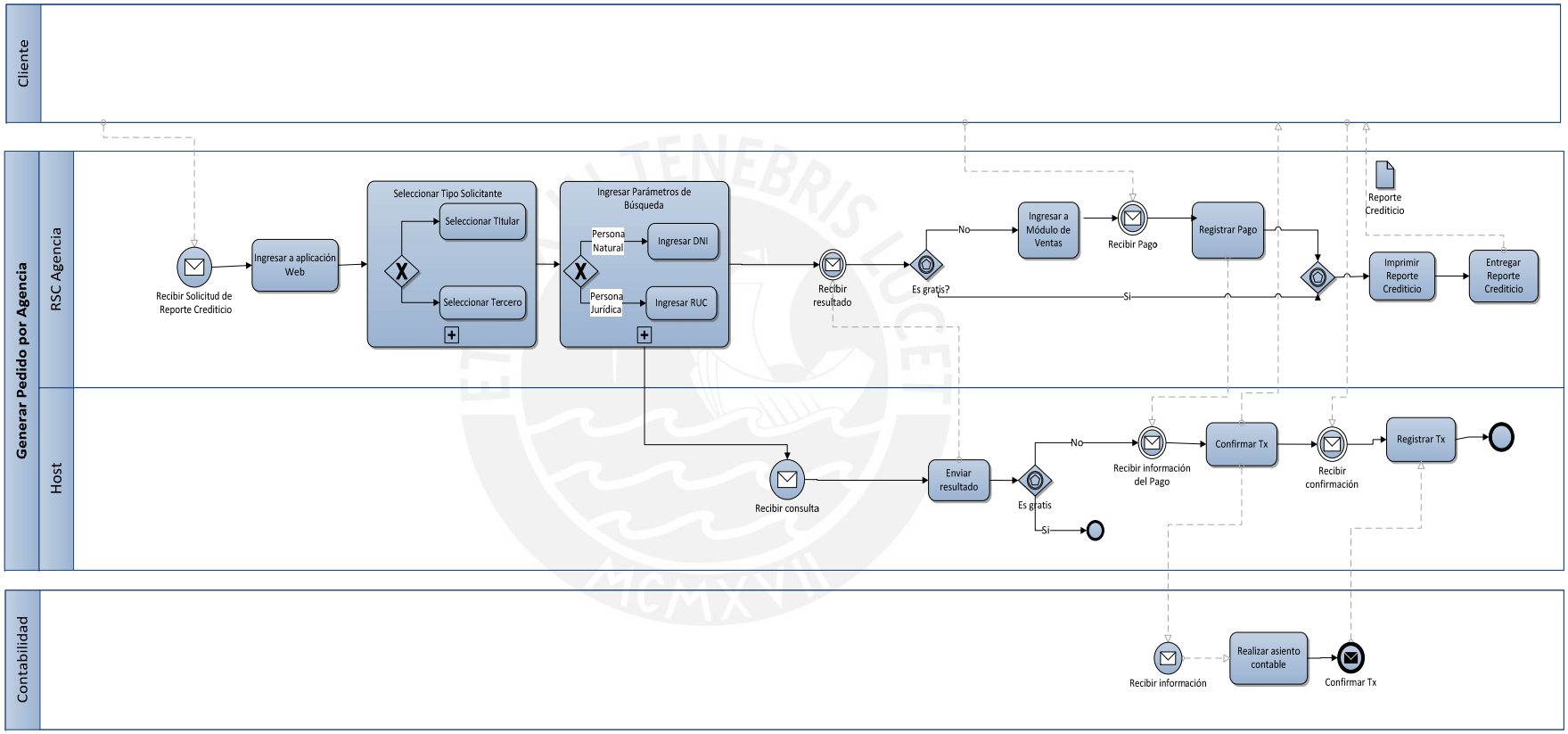
Anexo 4
Declaración de la Aplicabilidad

Anexo 1
Modelamiento BPM

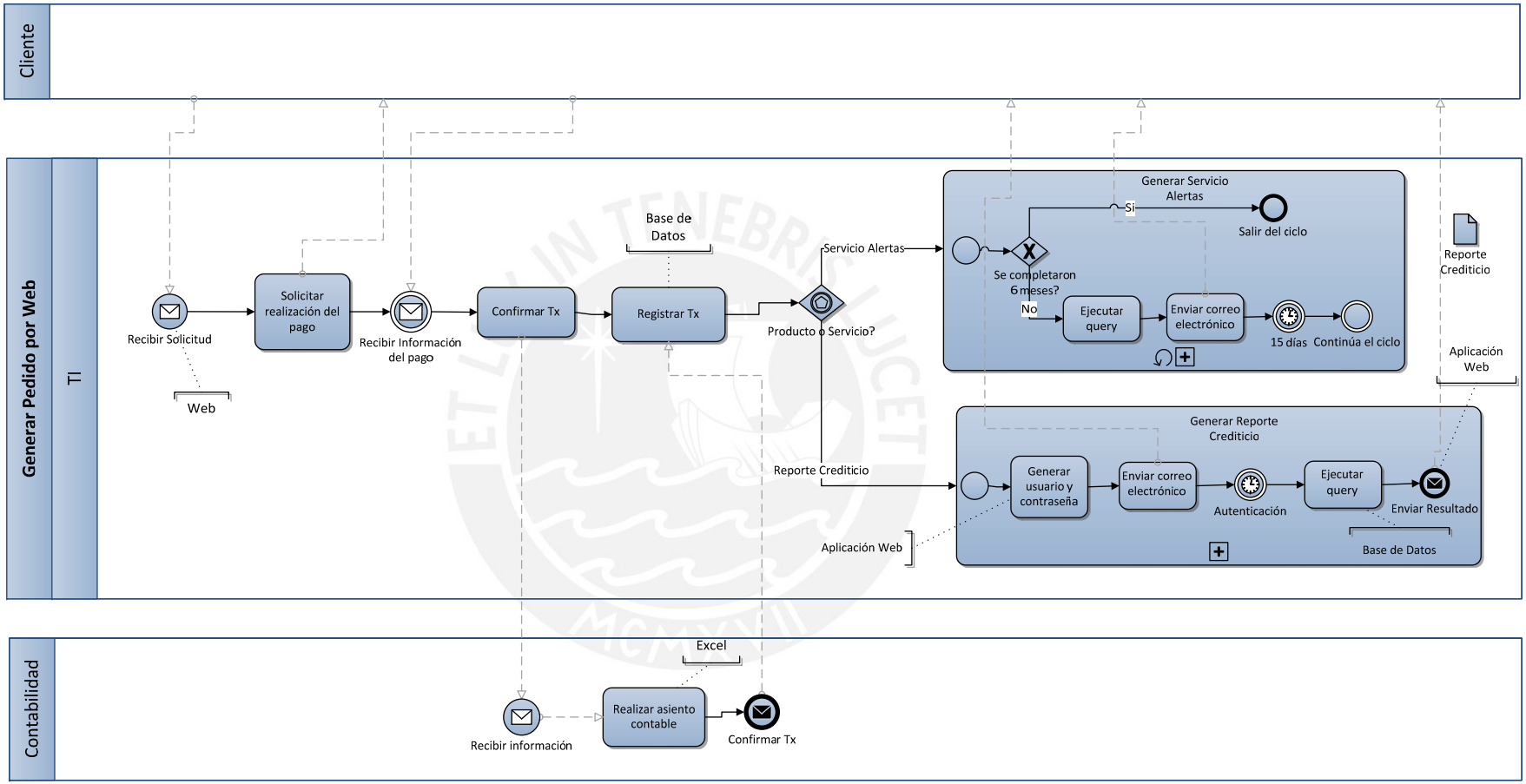
1. Compra y Venta de Productos



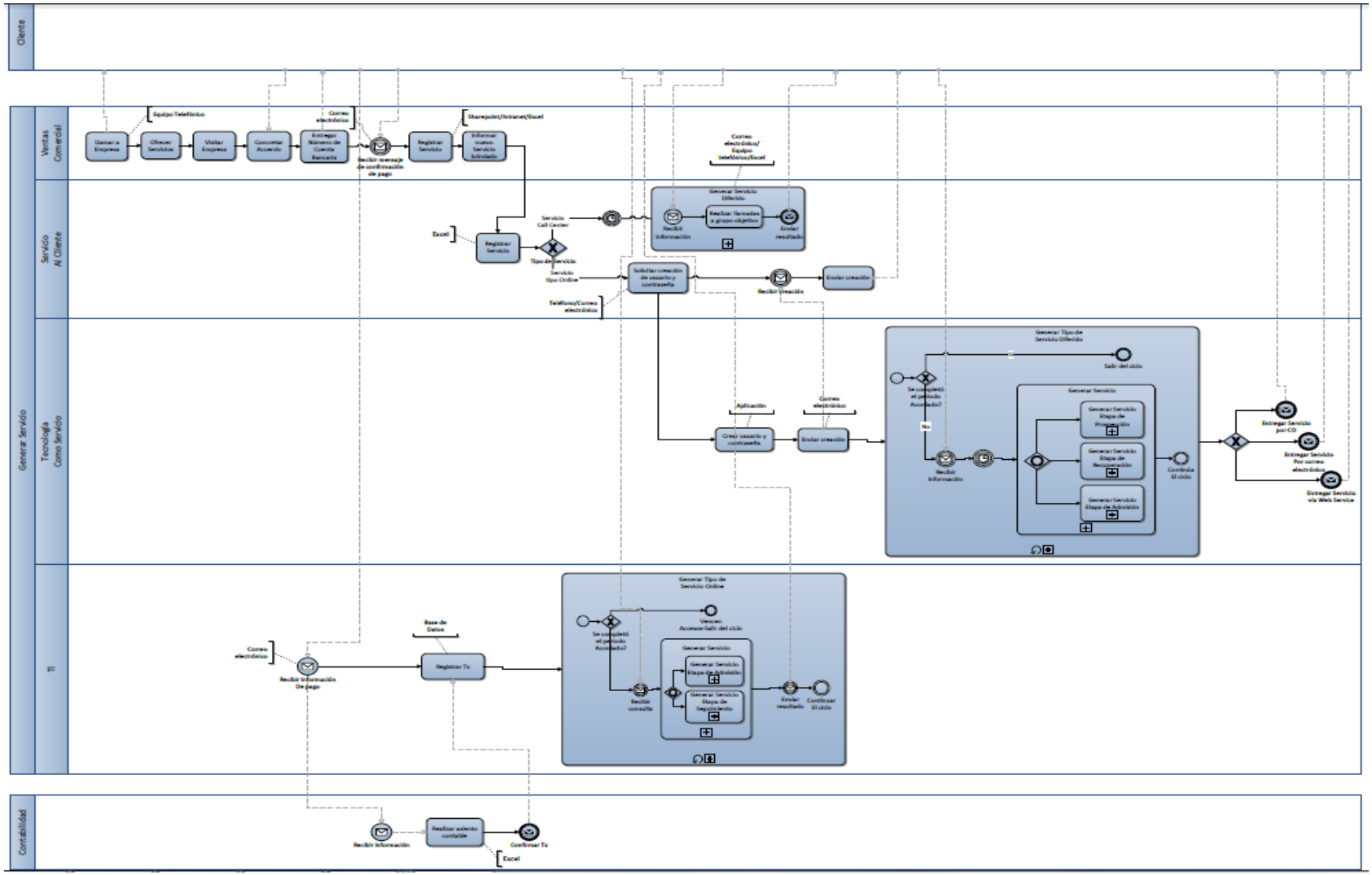
2. Venta por Agencia



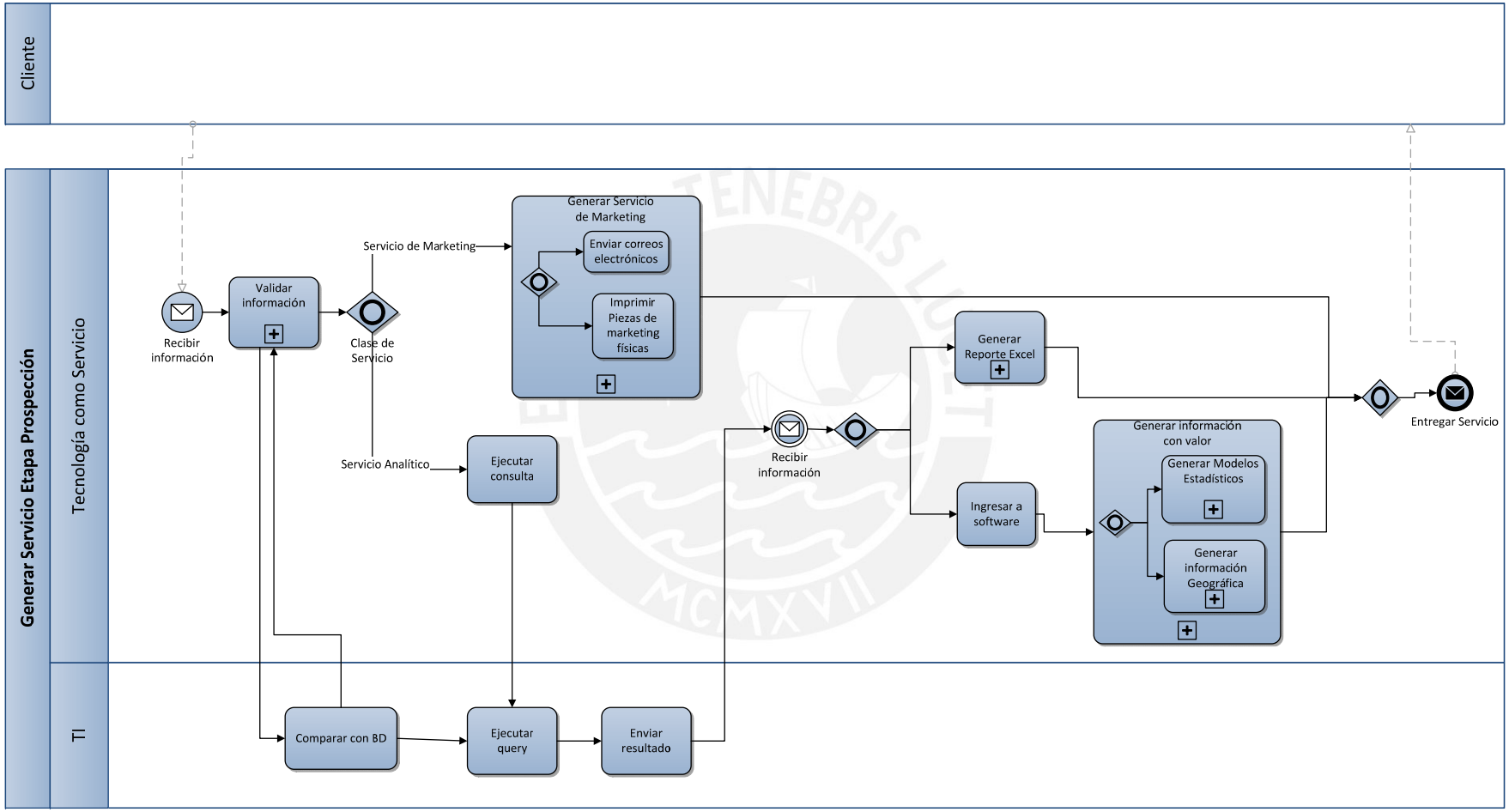
3. Venta por Web



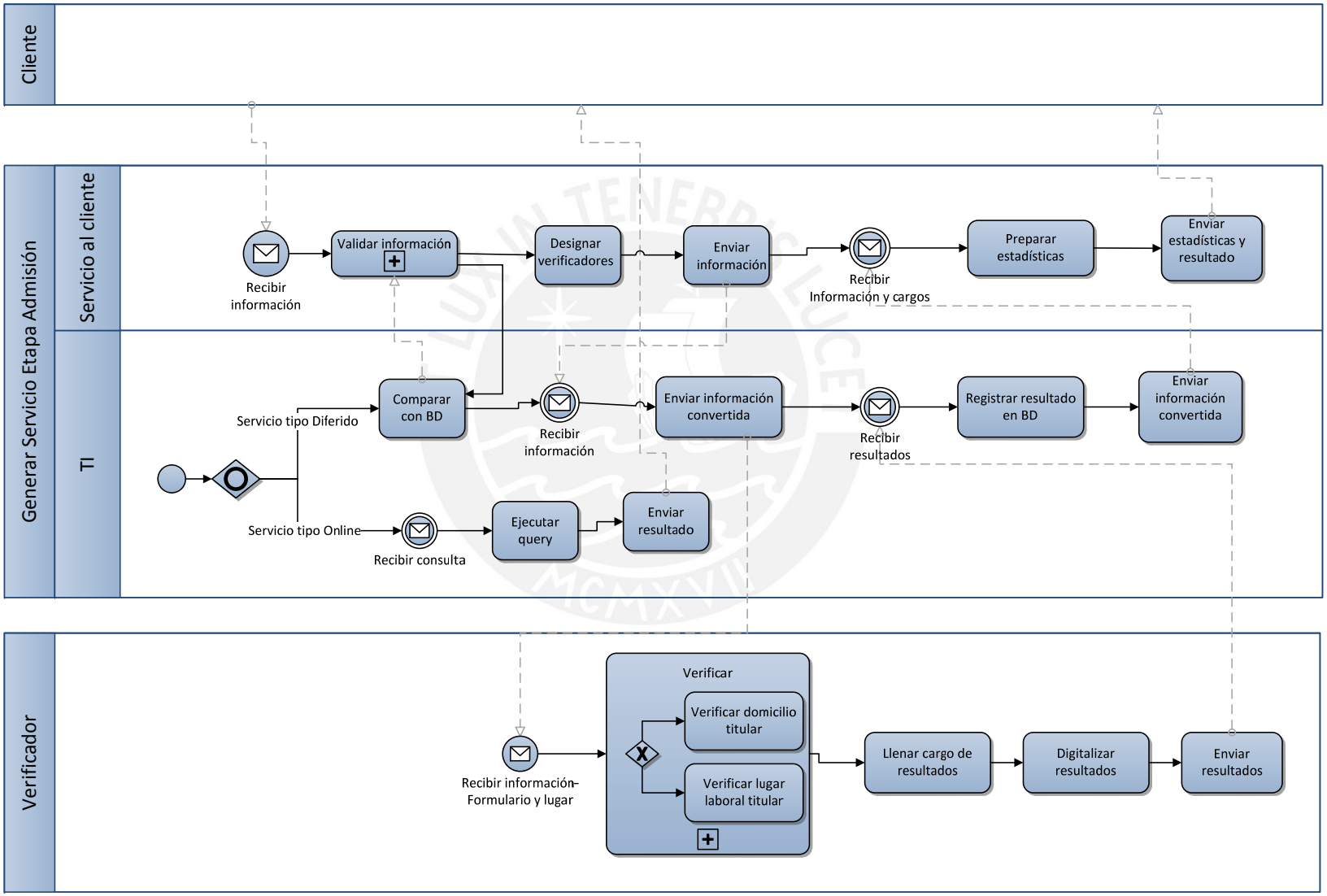
4. Venta de Servicios Complementarios a Empresas



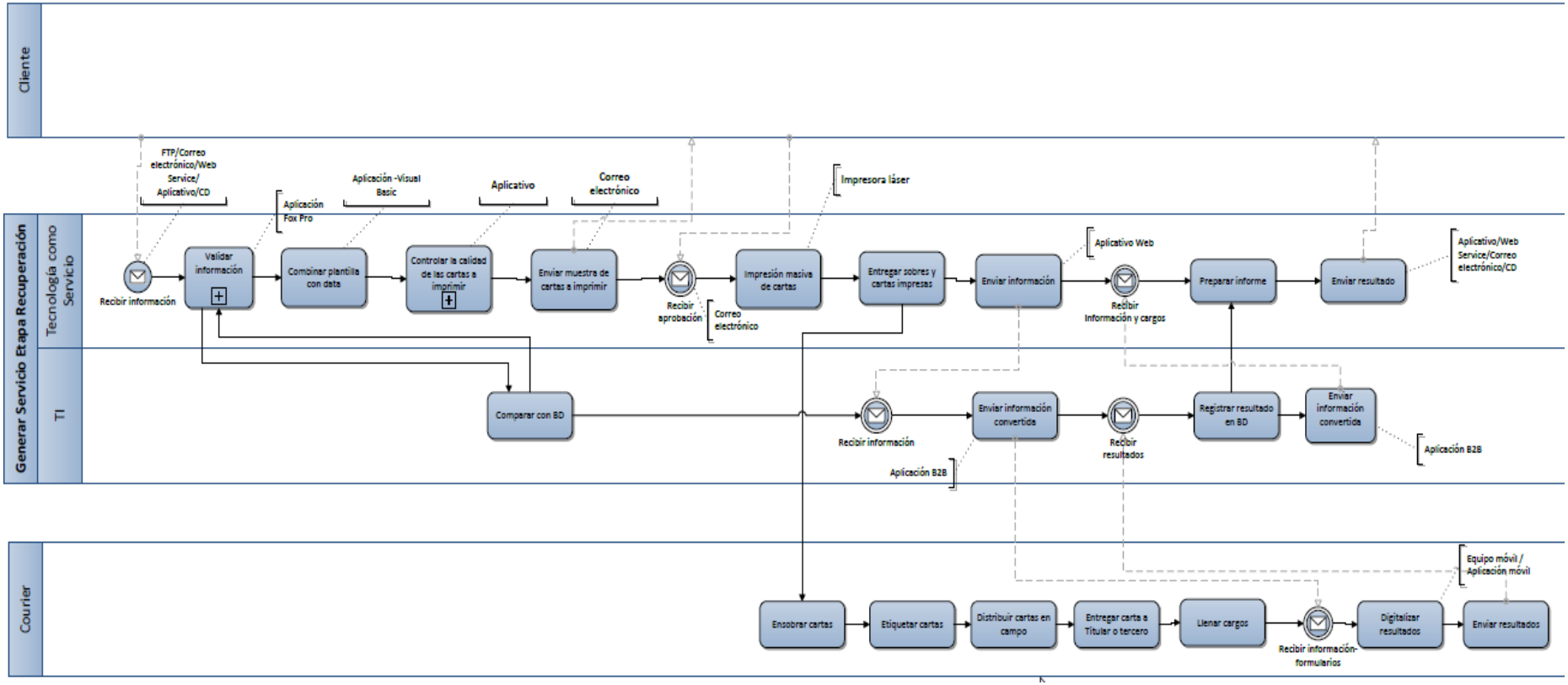
5. Generar Servicio Etapa Prospección



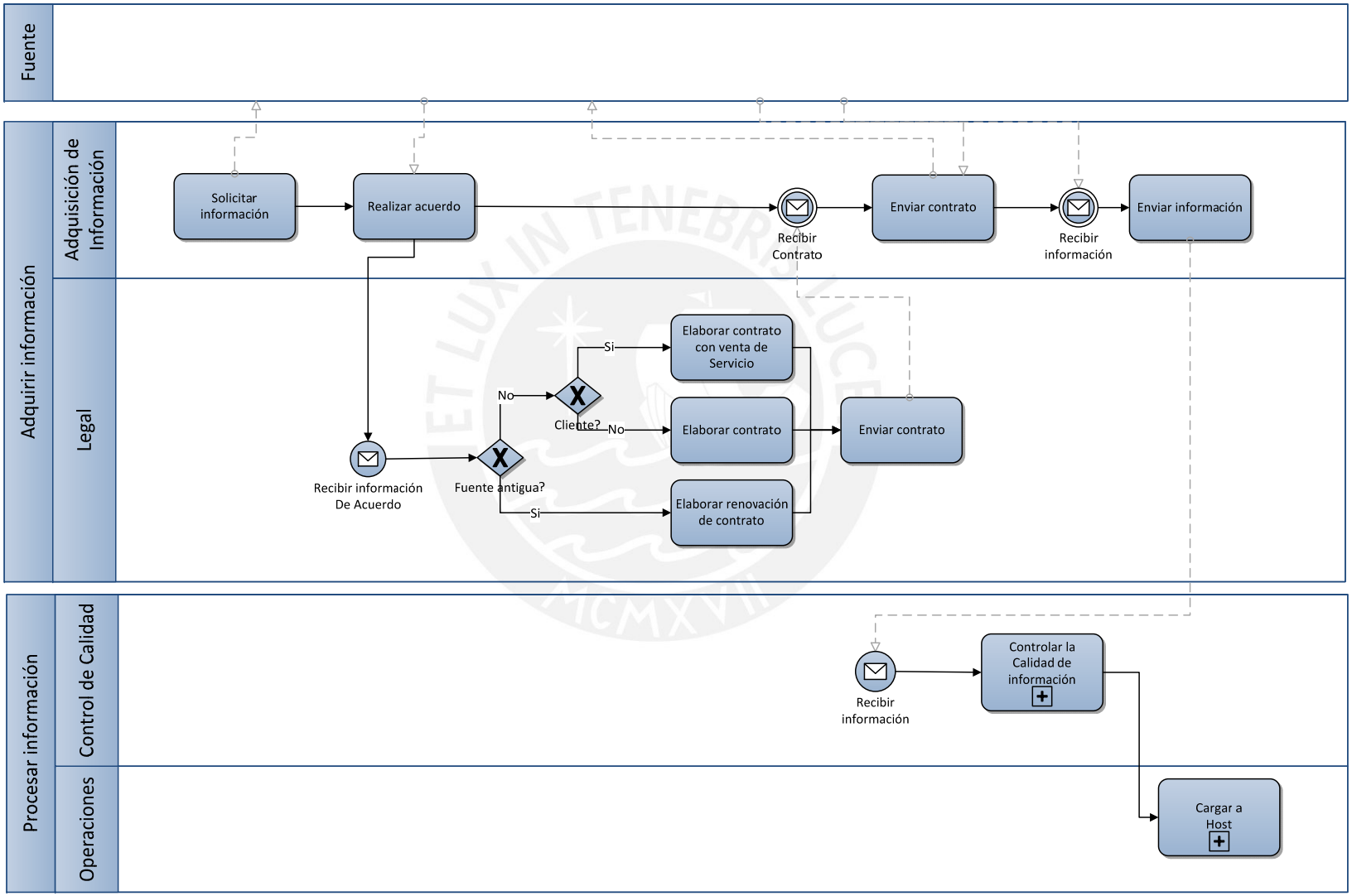
6. Generar Servicio Etapa Admisión



7. Generar Servicio Etapa Recuperación



8. Adquirir información



Anexo 2

Identificación y Valoración de Activos

1. Activos en el Proceso de Venta por Agencia

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Representantes de Servicio al Cliente (RSC)	Encargados de atender a los Titulares o Terceros que llegan a la Agencia por el Reporte Crediticio	Ingresar Aplicación Web	Generar Reporte Crediticio por Agencia	Soporte	Si
		Seleccionar Tipo de Solicitante	Generar Reporte Crediticio por Agencia	Soporte	Si
		Ingresar parámetros de búsqueda	Generar Reporte Crediticio por Agencia	Soporte	Si
		Ingresar a Módulo de Ventas	Generar Reporte Crediticio por Agencia	Soporte	Si
		Registrar Pago de Reporte Crediticio	Generar Reporte Crediticio por Agencia	Soporte	Si
		Imprimir Reporte Crediticio	Generar Reporte Crediticio por Agencia	Soporte	Si
		Entregar reporte Crediticio	Generar Reporte Crediticio por Agencia	Soporte	Si

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Aplicación Web para la Generación de Reportes Crediticios	Aplicación Web utilizada por los RSC para generar los Reportes Crediticios Online	Procesar información	Generar Reporte Crediticio por Agencia	Soporte	No
		Enviar Consulta a Host	Generar Reporte Crediticio por Agencia	Soporte	No
		Enviar información a cliente	Generar Reporte Crediticio por Agencia	Soporte	No
		Registrar Transacción	Generar Reporte Crediticio por Agencia	Soporte	No
PC	Utilizada por cada RSC	Ingresar aplicación Web	Generar Reporte Crediticio por Agencia	Soporte	SI
Reporte Crediticio	Reporte con el historial crediticio del Titular o persona consultada	Generar Reporte Crediticio	Generar Reporte Crediticio por Agencia	Primario	Si
		Entregar reporte Crediticio	Generar Reporte Crediticio por Agencia	Primario	Si
Impresora	Utilizada para la impresión de Reportes	Imprimir Reporte Crediticio	Generar Reporte Crediticio por Agencia	Soporte	Si
Voucher de Pago por Reporte Crediticio	Es el voucher que comprueba el pago de un Reporte Crediticio por un tercero	Registrar Pago de Reporte Crediticio	Generar Reporte Crediticio por Agencia	Soporte	Si
		Ingresar a Módulo de Ventas	Generar Reporte Crediticio por Agencia	Soporte	Si
Recibo	Comprobante de Pago	Registrar Pago de Reporte Crediticio	Generar Reporte Crediticio por Agencia	Soporte	Si

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
POS	Medio para realizar pagos	Registrar Pago de Reporte Crediticio	Generar Reporte Crediticio por Agencia	Soporte	Si
		Ingresar a Módulo de Ventas	Generar Reporte Crediticio por Agencia	Soporte	Si
Sistema Contable	Aplicación utilizada para registrar el pago de Reporte Crediticio	Registrar Pago de Reporte Crediticio	Generar Reporte Crediticio por Agencia	Soporte	No
		Ingresar a Módulo de Ventas	Generar Reporte Crediticio por Agencia	Soporte	No
Manual de Uso de Aplicación Web para la generación del Reporte Crediticio	Manual que ayuda a los RSCs en el uso de la aplicación	Ingresar aplicación Web	Generar Reporte Crediticio por Agencia	Primario	Si
Supervisor	Encargado de supervisar las actividades de los RSCs		Generar Reporte Crediticio por Agencia	Soporte	Si
Cámaras de vigilancia	Cámaras ubicadas dentro de la Agencia con el objetivo de grabar, detectar movimientos y actividades irregulares.		Generar Reporte Crediticio por Agencia	Soporte	Si
Antivirus	Programa utilizado por todas las PCs de la Agencia para la detección y prevención de *malware* .		Generar Reporte Crediticio por Agencia	Soporte	No

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Plataforma que soporta la aplicación Web	Sistema Operativo utilizado por las PCs de la Agencia.	Seleccionar Tipo Solicitante	Generar Reporte Crediticio por Agencia	Soporte	No
		Enviar Consulta	Generar Reporte Crediticio por Agencia	Soporte	No
		Ingresar parámentros de búsqueda	Generar Reporte Crediticio por Agencia	Soporte	No
		Confirmar Tx	Generar Reporte Crediticio por Agencia	Soporte	No
Base de Datos utilizada por la aplicación web	Alamacena las txs realizadas por los RSCs	Consultar BD	Generar Reporte Crediticio por Agencia	Soporte	No
		Ejecutar Query			
		Registrar Tx			
Personal Contabilidad	Encargado de la contabilidad que incluyen las ventas de Reportes Crediticios	Realizar Asiento contable	Generar Reporte Crediticio por Agencia	Soporte	Si
Personal de Soporte	Encargados de brindar soporte en caso de incidentes con el propósito de mantener operativos los servicios.		Generar Reporte Crediticio por Agencia	Soporte	Si
Oficina Agencia	Espacio en donde se realizan una parte de las operaciones y actividades de la Central de Riesgo		Generar Reporte Crediticio por Agencia	Primario	Si
Servidor Firewall	Encargado de bloquear el acceso no autorizado		Generar Reporte Crediticio por Agencia	Primario	Si
Servidor de aplicaciones	Almacena las principales aplicaciones, entre ellas la aplicación Web utilizada para emitir el reporte crediticio en Agencia		Generar Reporte Crediticio por Agencia	Primario	Si
Servidor de Base de datos	Cuya plataforma soporta la Base de datos de la Aplicación Web		Generar Reporte Crediticio por Agencia	Primario	Si

Activos del Proceso de Venta por Web

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Portal Web	Portal Web de la Central de Riesgo	Recibir Solicitud del Cliente	Generar Venta por Web	Soporte	No
		Solicitar Realización del pago	Generar Venta por Web		
		Recibir pago	Generar Venta por Web		
		Entregar Servicio de Alarmas y Reporte Crediticio	Generar Venta por Web		
		Confirmar Tx	Generar Venta por Web		
Base de Datos de la aplicación Web	En donde se registran las ventas de los servicios brindados por la Web	Registrar Tx en BD	Generar Venta por Web	Soporte	No
Teller de Comunicación	Sw de Comunicación	Enviar resultado	Generar Venta por Web	Soporte	No
		Solicitar Realización del pago	Generar Venta por Web	Soporte	No
		Recibir información de pago	Generar Venta por Web	Soporte	No
Correo electrónico	Utilizado para el envío del servicio de Alertas, el cual informará al cliente sobre alguna modificación en su reporte crediticio	Entregar Servicio de Alertas	Generar Venta por Web	Soporte	No
		Enviar usuario y contraseña a cliente			
Servidor de Correo	Servidor de correo electrónico	Entregar Servicio de Alertas	Generar Venta por Web	Soporte	Si

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Servidor de Correo	Servidor de correo electrónico	Enviar usuario y contraseña a cliente	Generar Venta por Web	Soporte	Si
Aplicación Web para generar el Reporte Crediticio	Genera el historial crediticio de la persona o entidad a buscar	Entregar Reporte Crediticio	Generar Venta por Web	Soporte	No
		Generar usuario y contraseña para cliente	Generar Venta por Web	Soporte	No
Personal de Soporte	Encargado de brindar soporte en caso de incidencias.		Generar Venta por Web	Soporte	Si
Personal Contabilidad	Encargado de dar soporte a la aplicación	Realizar Asiento contable	Generar Reporte Crediticio por Agencia	Soporte	Si
Servidor Firewall	Encargado de bloquear el acceso no autorizado		Generar Venta por Web	Soporte	No

2. Activos en el Proceso de Ventas por Servicios Complementarios a Empresas

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Equipo Telefónico	Equipo utilizado por Call Center - Servicio al Cliente	Llamar a Empresa	Venta Servicios para Empresas	Soporte	Si
		Generar Servicio Diferido	Venta Servicios para Empresas		
		Enviar solicitud de creación	Venta Servicios para Empresas		
		Ofrecer Servicios	Venta Servicios para Empresas		
Personal Comercial-Ventas	Es aquella persona que visita la empresa para ofrecer servicios	Visitar Empresa	Venta Servicios para Empresas	Soporte	Si
		Concretar acuerdo	Venta Servicios para Empresas	Soporte	Si
		Entregar número de cuenta bancaria	Venta Servicios para Empresas	Soporte	Si
Correo electrónico	Utilizado para el envío del servicio de tipo diferido y recepción de información	Recibir mensaje de confirmación de Pago	Venta Servicios para Empresas	Soporte	No
		Solicitar usuario y contraseña	Venta Servicios para Empresas		
		Entregar servicio por correo electrónico	Venta Servicios para Empresas		
		Enviar solicitud de creación	Venta Servicios para Empresas		
		Enviar creación a cliente	Venta Servicios para Empresas		

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
CD encriptado	Utilizado para el envío del servicio de tipo Diferido	Entregar Servicio po CD	Venta Servicios para Empresas	Soporte	Si
Servidor de Correo	Servidor de correo electrónico	Entregar servicio por correo electrónico	Venta Servicios para Empresas	Soporte	Si
		Recibir mensaje de confirmación de Pago	Venta Servicios para Empresas	Soporte	Si
		Enviar solicitud de creación	Venta Servicios para Empresas	Soporte	Si
		Solicitar usuario y contraseña	Venta Servicios para Empresas	Soporte	Si
Personal Operadores	Encargados de realizar las llamadas a las respectivas entidades	Llamar a Empresa	Venta Servicios para Empresas	Soporte	Si
		Generar Servicio Diferido	Venta Servicios para Empresas	Soporte	Si
		Ofrecer Servicios	Venta Servicios para Empresas	Soporte	Si

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Servidores de Base de Datos	En el cual se almacenan las Base de Datos de las aplicaciones.	Registrar Tx en BD	Venta Servicios para Empresas	Soporte	No
Servidores de Archivos	Donde se almacenan los archivos de la Organización	Generar tipo de servicio Diferido	Venta Servicios para Empresas	Soporte	No
Intranet de la Central de Riesgo	Intranet de la Central de Riesgo	Registrar servicio	Venta Servicios para Empresas	Soporte	No
Medios de Almacenamiento	Unidades de almacenamiento: USB, CDs, DVDs	Generar tipo de servicio Diferido	Venta Servicios para Empresas	Soporte	Si
FAX	Uso interno de la organización		Venta Servicios para Empresas	Soporte	Si
Infraestructura de red	Red de la Central de Riesgo		Venta Servicios para Empresas	Soporte	Si
Dominio Organizativo	Dominio Virtual		Venta Servicios para Empresas	Soporte	No

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Edificio	Espacio en donde se realizan las operaciones y actividades de la Central de Riesgo		Venta Servicios para Empresas	Soporte	Si
Impresora	Para uso interno de la oficina		Venta Servicios para Empresas	Soporte	Si
Personal de Mantenimiento	Encargados dela limpieza de escritorios y edificio		Venta Servicios para Empresas	Soporte	Si
Personal Contabilidad	Encargado de llevar la contabilidad que incluyen las ventas de Servicios Complementarios	Realizar Asiento contable	Venta Servicios para Empresas	Soporte	Si
Personal de TI	Personal encargado de generar la información con valor como servicio	Enviar creación	Venta Servicios para Empresas	Primario	Si
		Crear usuario y contraseña	Venta Servicios para Empresas	Primario	Si
		Entregar servicio por CD	Venta Servicios para Empresas	Primario	Si
		Entregar servicio por correo electrónico	Venta Servicios para Empresas	Primario	Si
		Entregar servicio vía WebService	Venta Servicios para Empresas	Primario	Si
		Generar tipo de servicio Diferido	Venta Servicios para Empresas	Primario	Si

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Personal Servicio al Cliente	Encargados de conversar directamente con el Cliente	Solicitar creación de usuario y contraseña	Venta Servicios para Empresas	Soporte	Si
		Enviar creación a cliente	Venta Servicios para Empresas	Soporte	Si
		Recibir creación	Venta Servicios para Empresas	Soporte	Si
Aplicación Web de Seguimiento Online	Software el cual, a través de la identificación y monitoreo brinda un seguimiento a la cartera de clientes de las empresas	Generar Servicio tipo online	Venta Servicios para Empresas	Soporte	No
Sistema de decisiones	Sistema experto para verificar la admisión de un titular a un crédito mediante su score crediticio	Generar Servicio tipo online	Venta Servicios para Empresas	Soporte	No
Base de Datos	Se registrará las txs de las ventas de servicios	Registrar Tx en BD	Venta Servicios para Empresas	Soporte	No
Web Service	Utilizada para la comunicación de apliacaciones Web	Entregar servicio vía WebService	Venta Servicios para Empresas	Soporte	No
Personal de Soporte	Encargado de dar soporte a Hw y Sw dentro de la Organización		Venta Servicios para Empresas	Soporte	Si

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Laptop	Para el uso interno, en especial por el personal de TI		Venta Servicios para Empresas	Soporte	Si
Red inalámbrica	Conexión Inalámbrica		Venta Servicios para Empresas	Soporte	No
Red Telefónica	Red de telefonía de la Organización		Venta Servicios para Empresas	Soporte	Si
Enrutador	Routers utilizados para el intercambio de información		Venta Servicios para Empresas	Soporte	Si
Zonas de acceso reservado	Zonas restringidas a personal específico dentro de la Central		Venta Servicios para Empresas	Soporte	Si
Reportes Excel del Servicio Complementario brindado	Documento que contiene la información de valor para el cliente	Entregar Servicio	Venta Servicios para Empresas	Soporte	Si

3. Activos en el Proceso de Generar Servicio en la Etapa de Prospección

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Documento Excel de Servicios brindados - Microsoft Excel 2007	Documento en donde están registrados los actuales servicios		Generar Servicios Etapa Prospección	Soporte	No
Correo electrónico	A través del cual llega la información del cliente y se le envía el servicio.	Recibir información	Generar Servicios Etapa Prospección	Soporte	No
		Entregar servicio	Generar Servicios Etapa Prospección		
Aplicación Web	A través del cual llega la solicitud del cliente	Recibir información	Generar Servicios Etapa Prospección	Soporte	No
Base de Datos	Registra las tx para las ventas de Servicios	Comparar con BD	Generar Servicios Etapa Prospección	Soporte	No
		Ejecutar Query	Generar Servicios Etapa Prospección		
Documento Excel Reporte Servicios de Prospección	Reporte entregado al cliente como Servicio	Generar Reporte Excel	Generar Servicios Etapa Prospección	Soporte	No
Aplicación para generar Modelos Estadísticos	Estadísticas e indicadores en base a reglas entregadas por el cliente	Ingresar a Sw	Generar Servicios Etapa Prospección	Soporte	No
		Generar información con valor	Generar Servicios Etapa Prospección	Soporte	No
		Generar Modelos estadísticos	Generar Servicios Etapa Prospección	Soporte	No

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Aplicación Georeferenciada	Aplicación utilizada para la etapa de prospección, mide el mercado considerando la ubicación geográfica de la población objetivo del cliente	Ingresar a Sw	Generar Servicios Etapa Prospección	Soporte	No
		Generar información con valor	Generar Servicios Etapa Prospección	Soporte	No
		Generar Información geográfica	Generar Servicios Etapa Prospección	Soporte	No
Brochure	Piezas que se generan como servicio de marketing para el cliente	Generar piezas de marketing físicas	Generar Servicios Etapa Prospección	Primario	Si
CD encriptado	Cd con información encriptada	Enviar información	Generar Servicios Etapa Prospección	Soporte	No
Web Service	Utilizado para la recepción de solicitudes. Comunicación entre la aplicación del cliente y la aplicación de la Central de Riesgo.	Recibir información	Generar Servicios Etapa Prospección	Soporte	No
Manual de uso de Aplicación para generar Modelos Estadísticos	Utilizado para el uso de la aplicación Modelos Estadísticos	Generar Modelos estadísticos	Generar Servicios Etapa Prospección	Soporte	Si

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Manual de uso de Aplicación Georeferenciada	Utilizado para el uso de la aplicación Aplicación Georeferenciada	Generar Información geográfica	Generar Servicios Etapa Prospección	Soporte	Si
Personal de Tecnología como Servicio	Encargado de brindar los servicios diferidos.	Enviar correos electrónicos	Generar Servicios Etapa Prospección	Primario	Si
		Ejecutar consultas	Generar Servicios Etapa Prospección	Primario	Si
		Validar información	Generar Servicios Etapa Prospección	Primario	Si
		Recibir información	Generar Servicios Etapa Prospección	Primario	Si
		Generar reporte Excel	Generar Servicios Etapa Prospección	Primario	Si
		Ingresar a Sw	Generar Servicios Etapa Prospección	Primario	Si
		Generar información con valor	Generar Servicios Etapa Prospección	Primario	Si
		Generar servicio de Marketing	Generar Servicios Etapa Prospección	Soporte	Si
Personal de TI	Encargado del desarrollo y mejora en tecnologías de información tales como aplicaciones de la Empresa.		Generar Servicios Etapa Prospección	Soporte	Si

4. Activos en el Proceso de Generar Servicio en la Etapa de Recuperación

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Correo electrónico	A través del cual se recibe las solicitudes de los clientes y se envía el servicio solicitado	Recibir Información	Generar Servicios Etapa Recuperación	Soporte	No
		Enviar información	Generar Servicios Etapa Recuperación	Soporte	
Documentos Excel de gestión	Documento el cual contiene los indicadores de cartas entregadas y sin entregar a los titulares	Enviar información	Generar Servicios Etapa Recuperación	Soporte	No
Aplicación para control de calidad de la data	Mediante el cual se realiza el control de calidad de la información recibida	Validar Información	Generar Servicios Etapa Recuperación	Soporte	No
		Combinación de plantilla con data	Generar Servicios Etapa Recuperación	Soporte	No
		Controlar la calidad de cartas	Generar Servicios Etapa Recuperación	Soporte	No
Base de Datos	Registra las tx para las ventas de Servicios	Enviar información convertida	Generar Servicios Etapa Recuperación	Soporte	No
		Comparar con BD	Generar Servicios Etapa Recuperación	Soporte	No
		Registrar resultado	Generar Servicios Etapa Recuperación	Soporte	No

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Impresoras	Utilzada para brindar el Servicio de entrega de cartas	Imprimir masivamente cartas	Generar Servicios Etapa Recuperación	Soporte	Si
Paquetes de Cartas de Cobranza	Son notificaciones a los clientes que tienen mora, ayudando a agilizar la conbranza	Imprimir masivamente cartas	Generar Servicios Etapa Recuperación	Primario	Si
Couriers	Personas que realizan la entrega de las cartas	Distribuir cartas a titulares o terceros	Generar Servicios Etapa Recuperación	Soporte	Si
		Ensobrar cartas	Generar Servicios Etapa Recuperación	Soporte	Si
		Etiquetar cartas	Generar Servicios Etapa Recuperación	Soporte	Si
		Llenar cargo de resultados	Generar Servicios Etapa Recuperación	Soporte	Si
		Digitalizar resultados	Generar Servicios Etapa Recuperación	Soporte	Si
		Enviar resultados	Generar Servicios Etapa Recuperación	Soporte	Si
Documentos de Cargo	Formatos de registro de los resultados del servicio brindado	Recibir Información y cargos	Generar Servicios Etapa Recuperación	Soporte	Si
		Llenado de Cargo de resultados	Generar Servicios Etapa Recuperación	Soporte	Si

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Equipo móvil	Se utilizan para enviar información del número de cartas entregadas por courier	Enviar resultados	Generar Servicios Etapa Recuperación	Soporte	SI
		Digitalizar resultados	Generar Servicios Etapa Recuperación	Soporte	SI
		Recibir información-formularios	Generar Servicios Etapa Recuperación	Soporte	SI
Aplicación B2B	Aplicaciones utilizadas en los equipos móviles que se comunican con las aplicaciones de la Organización.	Enviar información convertida	Generar Servicios Etapa Recuperación	Soporte	No
CD encriptado	CD encriptado con la información	Enviar información	Generar Servicios Etapa Recuperación	Soporte	Si
Personal TI	Encargado de brindar los servicios diferidos.	Validar información	Generar Servicios Etapa Recuperación	Primario	Si
		Combinar plantilla con data	Generar Servicios Etapa Recuperación	Primario	Si
		Controlar la calidad de cartas	Generar Servicios Etapa Recuperación	Primario	Si
		Imprimir masivamente cartas	Generar Servicios Etapa Recuperación	Primario	Si
		Entregar sobres, cartas impresas	Generar Servicios Etapa Recuperación	Primario	Si
		Recibir Información y cargos	Generar Servicios Etapa Recuperación	Primario	Si
		Preparar informe	Generar Servicios Etapa Recuperación	Primario	Si
		Enviar resultados	Generar Servicios Etapa Recuperación	Primario	Si

5. Activos en el Proceso de Generar Servicio en la Etapa de Admisión

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Web Service	Medio de comunicación entre las aplicaciones del cliente y la Central de Riesgo	Recibir información	Generar Servicio Etapa de Admisión	Soporte	No
		Enviar resultado	Generar Servicio Etapa de Admisión	Soporte	No
Servidor FTP	A través del cual el cliente puede enviar sus solicitudes	Recibir información	Generar Servicio Etapa de Admisión	Soporte	No
Aplicación Web de Verificaciones	Mediante la cual el cliente puede acceder y enviar sus solicitudes	Designar verificadores	Generar Servicio Etapa de Admisión	Soporte	No
		Enviar información a verificar	Generar Servicio Etapa de Admisión	Soporte	No
		Recibir información	Generar Servicio Etapa de Admisión	Soporte	No
Documento Excel Reporte	Documento el cual contiene los indicacodores de cartas entregadas y sin entregar a los titulares	Elaborar estadísticas	Generar Servicio Etapa de Admisión	Soporte	No
Correo electrónico	Canales de entrega de sevicio al cliente	Enviar estadísticas y resultado	Generar Servicio Etapa de Admisión	Soporte	No
		Recibir información	Generar Servicio Etapa de Admisión	Soporte	No

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
CD encriptado	Canales de entrega de sevicio al cliente	Enviar estadísticas y resultado	Generar Servicio Etapa de Admisión	Soporte	No
Sistema de decisiones	Sistema experto el cual se puede saber el conocimiento futuro del cliente mediante un score	Entregar resultado de consulta	Generar Servicio Etapa de Admisión	Soporte	No
		Ejecutar consulta	Generar Servicio Etapa de Admisión	Primario	No
Base de Datos	Registra las tx para las ventas de Servicios	Ejecutar query	Generar Servicio Etapa de Admisión	Soporte	No
		Comparar con BD	Generar Servicio Etapa de Admisión	Soporte	No
Portal Web	Por donde accede el cliente y se autentica para consultar la información de riesgo	Ingresar a aplicación Web	Generar Servicio Etapa de Admisión	Primario	No
		Digitalizar resultados			

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Equipo móvil	Se utilizan para enviar información de los datos domiciliarios y laborales de los titulares	Enviar resultados	Generar Servicio Etapa de Admisión	Soporte	SI
Aplicación B2B	Aplicación utilizada para enviar las aplicaciones móviles a los verificadores	Enviar información convertida	Generar Servicio Etapa de Admisión	Soporte	No
Personal Verificadores	Empleados quienes realizan trabajo de campo realizando verificaciones domiciliares y laborales	Verificar lugar de residencia titular	Generar Servicio Etapa de Admisión	Soporte	SI
		Llenar cargos	Generar Servicio Etapa de Admisión	Soporte	SI
		Digitalizar resultados	Generar Servicio Etapa de Admisión	Soporte	SI
Personal TI	Encargado de brindar los servicios diferidos.	Validar información	Generar Servicio Etapa de Admisión	Primario	Si
		Designar verificadores	Generar Servicio Etapa de Admisión	Primario	Si
		Enviar información para verificar	Generar Servicio Etapa de Admisión	Primario	Si
		Recibir resultados y cargos	Generar Servicio Etapa de Admisión	Primario	Si
		Preparar estadísticas	Generar Servicio Etapa de Admisión	Primario	Si

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Documento Cargo	Formatos de registro de los resultados del servicio brindado	Recibir Información y cargos	Generar Servicio Etapa de Admisión	Soporte	Si
		Llenar Cargo de resultados	Generar Servicio Etapa de Admisión	Soporte	Si

6. Activos en el Proceso de Adquirir Información

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Contrato	Contrato público o privado de acuerdo a la fuente, en donde se realiza el acuerdo de pago, envío de información y condiciones de servicio brindado a la fuente	Realizar acuerdo público o privado con venta de Servicio	Comprar información	Primario	Si
		Realizar acuerdo público o privado	Comprar información	Primario	Si
		Elaborar contrato	Comprar información	Primario	Si
		Renovar acuerdo	Comprar información	Primario	Si
Correo electrónico	Utilizado para recibir información de la fuente	Recibir Información	Comprar información	Soporte	No
Cd encriptado	Utilizado para recibir información de la fuente	Recibir Información	Comprar información	Primario	Si
Web service	Utilizado para la comunicación entre la aplicación del cliente y la aplicación de la Central de Riesgo	Recibir Información	Comprar información	Soporte	No

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Portal Web	Por donde la fuente puede enviar información.	Recibir Información	Comprar información	Soporte	Si
Aplicación utilizada para el control de calidad de la información	Mediante el cual se recolecta la información y se realiza el control de calidad de la información recibida	Controlar la calidad de la información	Comprar información	Soporte	No
Cintas magnéticas - Back ups	Se realizan back ups periódicamente de la información enviada por las fuentes	Controlar la calidad de la información	Comprar información	Primario	Si
Base de Datos del sistema de Ventas	Registra las transacciones para las ventas de Servicios	Controlar la calidad de la información	Comprar información	Soporte	No

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Personal Mantenimiento	Realiza la limpieza de las oficinas		Comprar información	Soporte	Si
Archivos para cargar al host	Archivos recibidos por las fuentes	Cargar información al Host	Comprar información	Soporte	No
Host	El cual contiene toda la información de las fuentes	Cargar información al Host	Comprar información	Primario	No
Equipo telefónico	Medio de comunicación	Solicitar información	Comprar información	Soporte	Si
Documento Cotización	Documento presentado al cliente en donde están los servicios ofrecidos y sus respectivos precios	Realizar acuerdo	Comprar información	Soporte	No
Personal Legal	Encargados de elaborar los contratos	Recibir información de acuerdo	Comprar información	Soporte	Si
		Elaborar Contrato con venta de servicio	Comprar información	Soporte	Si
		Elaborar Contrato con venta de servicio	Comprar información	Soporte	Si
		Elaborar renovación de contrato	Comprar información	Soporte	Si

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Personal Operaciones	Personal encargado de subir al Host la información validada por Control de Calidad	Cargar a Host	Comprar información	Soporte	Si
Personal Control de Calidad	Personal encargado de validar la información a través del uso de aplicaciones	Controlar la calidad de la información	Comprar información	Soporte	Si
Documentos de Fuentes (Excel, txt, etc.)	Documentos los cuales contienen la información acerca de los titulares brindada por las fuentes	Información enviada por las fuentes	Comprar información	Primario	No
Intranet	Intranet de la compañía, medio en donde se recibe la información de clientes.	Información enviada por las fuentes	Comprar información	Primario	No
Sala de Servidores	Sala en donde se encuentran los servidores utilizados por la Compañía.		Comprar información	Primario	No

Activo	Descripción	Tarea	Proceso	Tipo	Tangible
Servidores de aplicación	Servidores los cuales soportan las aplicaciones encargadas de gestionar la información.	Cargar a Host	Comprar información	Soporte	Si
		Control de Calidad de Información	Comprar información	Soporte	Si
		Recibir información de fuentes (Procesar)	Comprar información	Soporte	Si
Intranet	Intranet de la Compañía, medio en donde se recibe la información de clientes.	Información enviada por las fuentes	Comprar información	Primario	No
UPS	Proporciona energía durante apagones.	Cargar a Host	Comprar información	Primario	Si
Personal Adquisición de Información	Personal encargado de negociar con las fuentes la periodicidad del envío de información y el medio de envío	Solicitar información	Comprar información	Primario	Si
		Recibir contrato	Comprar información	Primario	Si
		Enviar contrato a fuente	Comprar información	Primario	Si
		Enviar información de fuente	Comprar información	Primario	Si
		Realizar acuerdo	Comprar información	Primario	Si

Anexo 2
Valoración de Activos

ID	ACTIVO	CRITERIOS																													VALOR
		Disponibilidad										Integridad										Confidencialidad									
		1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	
A01	Representantes de Servicio al Cliente (RSC)	3	3	3	3	3	0	3	0	3	0	3	3	1	3	3	0	3	3	0	0	1	1	1	3	3	3	3	3	0	0	58
A02	Aplicación Web - Reporte Crediticio Online	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	1	3	1	3	3	3	3	3	3	3	86
A03	PC	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	3	3	3	81
A04	Reporte Crediticio	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	90
A05	Impresora	1	3	2	3	2	0	0	0	3	3	0	3	2	3	2	0	0	0	3	3	0	0	0	3	3	3	3	3	3	0	51
A06	Voucher de Pago por Reporte Crediticio	0	3	1	1	1	0	3	0	0	3	0	1	0	3	3	0	3	0	0	3	0	1	0	3	3	0	3	0	0	3	38
A07	Aplicación Ventas	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	1	3	1	3	3	3	3	3	3	3	86
A08	Recibo	0	3	1	1	1	0	3	0	0	3	0	1	0	3	3	0	3	0	0	3	0	1	0	3	3	0	3	0	0	3	38
A09	POS	3	3	3	3	3	0	0	0	0	3	3	3	3	3	3	0	0	0	0	3	3	3	3	3	3	0	0	0	0	3	54
A10	Manual de Uso de Aplicación Web	0	3	0	3	3	0	3	3	3	3	0	3	0	3	3	0	3	3	3	3	0	0	0	3	3	0	3	3	0	3	57
A11	Supervisor de RSCs	1	1	1	2	2	0	1	3	1	0	2	2	2	2	2	0	0	3	2	0	2	2	2	2	2	0	0	3	2	0	42
A12	Cámaras de vigilancia	0	0	1	1	2	1	1	2	0	3	0	0	0	3	2	1	0	3	0	3	0	0	0	3	2	1	0	3	0	3	35
A13	Personal de soporte	3	3	3	3	3	0	3	0	3	0	3	3	1	3	3	0	3	3	0	0	1	1	1	3	3	3	3	3	0	0	58
A14	Antivirus	0	0	0	3	3	3	3	3	3	3	0	0	0	3	3	3	3	3	3	3	0	0	0	3	3	3	3	3	3	3	63
A15	Plataforma	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	0	0	0	3	3	0	3	3	3	3	78

ID	ACTIVO	CRITERIOS																														VALOR
		Disponibilidad										Integridad										Confidencialidad										
		1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	
A16	Base de Datos	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	0	0	0	3	3	0	3	3	3	3	78
A17	Portal Web	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	90
A18	Correo electrónico	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	90
A19	Servidor de Correo	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	90
A20	Equipo Telefónico	3	3	3	3	3	3	3	3	3	3	0	3	3	3	3	0	3	3	3	3	0	3	0	3	3	0	3	3	3	3	75
A21	Personal Comercial - Ventas	2	1	1	3	3	3	0	0	0	0	3	3	3	3	3	3	3	3	3	0	1	1	1	3	3	3	3	3	3	3	64
A22	CD encriptado	0	3	0	3	3	3	3	3	3	3	0	3	0	3	3	3	3	3	3	3	0	3	0	3	3	3	3	3	3	3	72
A24	Operadores	3	3	3	3	3	3	1	0	1	0	3	3	3	3	3	3	3	3	0	0	3	3	3	3	3	3	3	3	0	0	68
A25	Documentos Excel	0	1	0	3	1	3	1	0	0	3	0	1	0	3	3	3	3	0	3	3	0	1	0	3	3	3	3	0	3	3	50
A26	Servidores de Base de Datos	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	90
A27	Servidores de Archivos	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	90
A28	Intranet de la Central de Riesgo	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	90
A29	Medios de Almacenamiento	3	3	3	3	3	0	3	0	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	3	3	3	78
A30	FAX	0	0	0	1	1	0	0	0	1	1	0	0	0	3	2	0	0	0	0	1	0	0	0	3	2	0	0	0	0	1	16
A31	Softwares de gestión de archivos	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	0	0	0	3	3	0	3	3	3	3	78
A32	Infraestructura de red	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	90
A33	Dominio Organizativo	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	90
A34	Edificio	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	90
A35	Oficina Agencia	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	90
A36	Impresora Industrial	1	3	2	3	2	0	0	0	3	3	0	3	2	3	2	0	0	0	3	3	0	0	0	3	3	3	3	3	3	0	51

ID	ACTIVO	CRITERIOS																													VALOR
		Disponibilidad										Integridad										Confidencialidad									
		1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	
A37	Personal de Mantenimiento	0	0	0	0	0	0	0	0	3	0	0	0	0	3	3	2	3	3	3	0	0	0	0	3	3	2	3	3	3	0	37
A38	Personal Contabilidad	0	0	3	3	3	3	1	0	1	0	0	3	3	3	3	3	3	3	3	0	0	3	3	3	3	3	3	3	3	0	62
A39	Aplicación Web de Seguimiento Online	3	3	1	3	3	3	3	0	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	79
A40	Documento Excel Reporte	1	3	0	3	3	3	3	0	3	0	3	3	1	3	3	3	3	3	3	3	3	3	1	3	3	3	3	3	3	3	75
A41	Aplicación para generar Modelos Estadísticos	3	3	1	3	3	3	3	0	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	79
A42	Aplicación Georeferenciada	3	3	1	3	3	3	3	0	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	79
A43	Brochures para Clientes	1	3	1	3	3	3	0	0	0	3	1	3	1	3	3	3	0	0	0	3	1	3	1	3	3	3	0	0	0	3	51
A44	Piezas de Marketing como servicio al Cliente	3	3	3	3	3	3	3	1	3	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	82
A45	Web Service	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	90
A46	Manual de uso de Aplicación para generar Modelos Estadísticos	0	3	0	3	3	0	3	3	3	3	0	3	0	3	3	0	3	3	3	3	0	0	0	3	3	0	3	3	0	3	57
A47	Manual de uso de Aplicación Aplicación Georeferenciada	0	3	0	3	3	0	3	3	3	3	0	3	0	3	3	0	3	3	3	3	0	0	0	3	3	0	3	3	0	3	57
A48	Personal de Tecnología de Información	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	87
A49	Personal de Tecnología como Servicio	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	87
A50	Aplicación Web de Preselección	3	3	1	3	3	3	3	0	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	79
A51	Aplicación para la depuración y enriquecimiento de Data	3	3	1	3	3	3	3	0	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	79

ID	ACTIVO	CRITERIOS																														VALOR
		Disponibilidad										Integridad										Confidencialidad										
		1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	
A52	Aplicación Visual Fox Pro	3	3	1	3	3	3	3	0	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	79
A54	Paquetes de Cartas de Cobranza	3	3	3	3	3	3	3	1	3	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	82
A55	Courier	1	0	0	0	0	0	0	0	3	0	0	0	0	3	3	2	3	3	3	0	0	0	0	3	3	2	3	3	3	0	38
A56	Cargo	1	3	3	3	3	3	3	3	3	0	3	3	2	3	3	1	3	3	0	0	3	3	2	3	3	1	3	3	0	0	67
A57	Equipo móvil	3	3	2	3	3	0	3	0	3	3	3	3	2	3	3	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3	81
A58	Aplicación B2B	3	3	1	3	3	3	3	0	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	79
A59	Servidor FTP	3	3	1	3	3	3	3	0	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	79
A60	Sistema de decisiones	3	3	1	3	3	3	3	0	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	79
A61	Verificadores	1	3	1	2	2	1	1	0	1	0	2	3	2	3	3	2	3	3	3	1	2	3	2	3	3	2	3	3	3	1	62
A62	Contrato	3	3	2	3	3	3	3	3	3	1	3	3	2	3	3	2	1	3	2	0	3	3	2	3	3	2	1	3	2	0	71
A63	Aplicación para el control de calidad de la información	3	3	1	3	3	3	3	0	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	79
A64	Cintas magnéticas - Back ups	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	2	3	3	3	3	88
A65	Base de Datos Microsoft Sql Server 2003	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	0	0	0	3	3	0	3	3	3	3	78
A66	Aplicación Visual Fox Pro Lenguaje de Programación	3	3	1	3	3	3	3	0	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	79
A67	Base de datos de la aplicación Control de calidad	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	90
A70	Host	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	90
A71	Documentos Excel para el cliente	0	1	0	3	1	3	1	0	0	3	0	1	0	3	3	3	3	0	3	3	0	1	0	3	3	3	3	0	3	3	50

ID	ACTIVO	CRITERIOS																												VALOR
		Disponibilidad										Integridad										Confidencialidad									
		1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10	
A73	Documento Cotización	0	1	0	3	1	3	1	0	0	3	0	1	0	3	3	3	3	0	3	3	0	1	0	3	3	3	3	0	3	3	50
A74	Aplicación de Verificaciones	3	3	1	3	3	3	3	0	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	79
A75	Personal Servicio al Cliente	2	1	1	3	3	3	0	0	0	0	3	3	3	3	3	3	3	3	3	0	1	1	1	3	3	3	3	3	3	3	64
A76	Personal Legal	2	1	1	3	3	3	0	0	0	0	3	3	3	3	3	3	3	3	3	0	1	1	1	3	3	3	3	3	3	3	64
A77	Personal Adquisición de información	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	87
A78	Personal Operaciones	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	87
A79	Personal Control de Calidad	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	87
A80	Laptop	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	3	3	3	3	3	3	3	3	0	3	3	3	3	81
A84	Sala de Servidores	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	2	3	3	3	3	87
A86	Entrada Oficinas	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	2	3	3	3	3	87

Anexo 3

1. Matriz de Riesgos: Generar Venta por Agencia

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A01	Representates de Servicio al Cliente (RSC)	Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal	IDR01	Falta de disponibilidad del personal encargado de uno de los procesos core del negocio	Operativa impactada de los procesos de negocio	Impacto en productividad del negocio	Por falta de disponibilidad de personal de la Agencia, se afecte la operativa de la entrega de Reportes Crediticios, por ende la productividad del negocio	4	1	4
			Procedimientos inadecuados de contratación	Destrucción de equipos o medios	IDR02	Contratación de Personal incompetente con desconocimiento o incumpla las normas, políticas y criterios de seguridad de la Central	Incumplimiento de normas	Vulnerabilidad de la Seguridad de la Organización	Debido a un inadecuado procedimiento de contratación, como la evidencia de antecedentes penales y policiales, desarrollo de pruebas de competencia, desconocimiento de las normas, políticas y criterios de seguridad de información, se incumplan las normas internas pudiendo generar debilidades y vulnerabilidades en la seguridad de la Central de Riesgo.	4	2	5
			Entrenamiento insuficiente en seguridad	Error en el uso	IDR03	Falta de capacitación a personal	Error en el uso de aplicativos y Hardware	Indisponibilidad y/o falta de integridad de información	Debido a un entrenamiento insuficiente en seguridad, el personal que tiene acceso a equipos que almacenan o procesan información crítica afecte la disponibilidad e integridad de la información.	4	2	5
				Uso no autorizado de equipo	IDR04	Inadecuados procedimientos de custodia	Acceso a personal no autorizado a equipos criticos	Indisponibilidad y/o falta de integridad de información	Personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio de la Central, pudiendo afectar la disponibilidad e integridad de la información.	5	2	6
			Uso incorrecto de software y hardware	Error en el uso	IDR05	Insuficientes politicas de proteccion	Mala manipulación de equipos y aplicativos, los cuales se encuentran desprotegidos	Atacantes externos aprovechen vulnerabilidades	Debido a insuficientes políticas de protección y falta de capacitación, los equipos se encuentren desprotegidos y se exploten vulnerabilidades, pudiendo afectar afectar la disponibilidad e integridad de la información.	5	3	7
			Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo	IDR06	Falta de políticas de uso de correo electrónico	Ataques informaticos a aplicaciones del negocio	Indisponibilidad y/o falta de integridad de las aplicaciones	Por falta de políticas del uso de correo electrónico, se produzcan ataques informáticos a aplicaciones del negocio, pudiendo provocar indisponibilidad y/o falta de integridad de las aplicaciones.	5	4	8
		Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR07	Inadecuadas políticas	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de registro y retiro de registro de usuario, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio de la Central, pudiendo afectar la integridad y/o disponibilidad de la información.	5	3	7

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A02	Aplicación Web Reporte Crediticio Online	Software	El aplicativo web contiene defectos o fallas en su desarrollo.	Mal funcionamiento del software	IDR 08	Inadecuados procesos de detección	Intentos no autorizados de acceso a información	Debido al Robo o fuga de información haya pérdidas financieras	Debido a un mal funcionamiento de algunos aplicativos web podrían haber intentos no autorizados de acceso que no sean detectados y se produzcan ataques informáticos, lo que conlleva a robo o fuga de información	5	3	7
				Abuso de derechos	IDR 09	Fallas en el aplicativo Web	Falla en los accesos	Imposibilidad de ejecutar labores	Debido a fallas en aplicativo web (por ejm: el personal podría no contar con accesos disponibles) se imposibiliten las labores cotidianas trayendo pérdidas financieras para la empresa e improductividad	4	2	5
			Falta de terminación de Sesión cuando se cierra el aplicativo.	Falsificación de derechos Abuso de derechos	IDR 10	Fallas en el aplicativo Web	Usuarios no autorizados ingresen al sistema	Falta de integridad y/o disponibilidad de la información	Debido a fallas de terminación de sesión del aplicativo Web, usuarios a quienes no le corresponden acceso, ingresen al sistema pudiendo afectar la integridad y/o disponibilidad de la información.	5	1	5
			Falta de mecanismos de autenticación e identificación de usuario	Falsificación de derechos	IDR 11	Falta de identificación de usuarios / logs insuficientes	Imposibilidad de identificar a usuario	No sea posible tomar acción correctiva	Debido a la falta de mecanismos de autenticación e identificación de usuarios / logs insuficientes, no sea posible identificar a usuario y por ende no sea posible tomar acción correctiva.	5	2	6
			Interfaz de usuario complicada	Error en el uso	IDR 12	Interfaz compleja	Error en el uso del aplicativo	Fuga y/o divulgación de la información	Debido a una interfaz complicada , no se realice correctamente la definición de los perfiles de accesos y por ende los usuarios tengan accesos de más o restringidos.	4	3	6
			Faltas de las pruebas de software	Abuso de derechos	IDR 13	Inadecuada gestión de accesos	Usuarios con mas accesos de los definidos inicialmente	Impacto en productividad del negocio	Debido a la falta de pruebas en el software traiga como consecuencia una inadecuada gestión de accesos y se otorguen mayores accesos a los usuarios de los que se definieron inicialmente, posibilitando el uso incorrecto de los mismos.	4	3	6
			Falta de documentación y actualización de dicha documentación	Error en el uso	IDR 14	Fallas en la gestión de la documentación	Información no disponible	Pérdida de Integridad en la información, fuga de información, divulgación	Por falta de documentación (manuales, procedimientos, reporte de turnos e indicadores de gestión), haya la posibilidad de fallas en el otorgamiento de accesos generando fuga de información	4	4	7
			Gestión deficiente de las contraseñas	Falsificación de derechos	IDR 15	Inadecuadas políticas de almacenamiento de passwords	Contraseñas maestras accesadas por personal no autorizado	Inadecuados niveles de servicio y/o fuga de información	Debido a inadecuadas políticas de almacenamiento de passwords, las contraseñas maestras sean accesadas por personal no autorizado, pudiendo afectar los niveles de servicio y/o provocar fuga de información.	5	4	8
			Falta de control eficaz del cambio Descargas y usos no controlados del aplicativo	Mal funcionamiento del aplicativo	IDR 16	Errores en la asignación de perfiles	Inadecuada segregación de funciones	Controles sin efectividad	Debido a un ineficiente control de cambios del aplicativo exista errores en la asignación de perfiles definidos para los roles del personal y por consiguiente no exista una adecuada segregación de funciones para los procesos de negocios de la Central de Riesgo, por lo que los controles de los procesos pierdan efectividad.	4	2	5
			Falta de protección física en las puertas y ventanas de la Agencia o edificación	Hurto	IDR 17	Falta de protección física	Robo	Pérdidas financieras	Debido a la falta de protección física en las puertas se produzca robo de información, fuga o divulgación lo que conlleve a pérdidas financieras	5	1	5
		Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de derechos	IDR 18	Errores en la baja de usuarios	Accesos a usuarios no autorizados	Robo y/o fuga de información	Debido a errores en el procedimiento de baja de usuarios, no se dé de baja o bloquee los accesos a un usuario que cambia de puesto de trabajo, posibilitando el robo y/o fuga de información.	5	4	8

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A03	PC	Hardware	Falta o insuficiencia en el acuerdo a nivel de servicio	Incumplimiento en el mantenimiento de los sistemas de información	IDR 19	Falta de mantenimiento del equipo	Imposibilidad de realizar las labores	Operativa impactada en los procesos de negocio	Falla en el funcionamiento de los aplicativos debido al incumplimiento del mantenimiento de la PC lo que podría generar un impacto en la productividad del negocio	5	3	7
			Susceptibilidad al polvo, suciedad	Corrosión, destrucción del equipo								
A04	Reporte Crediticio	Personal	Entrenamiento insuficiente en seguridad	Errores en el uso de aplicaciones o en el proceso	IDR 20	Falta de capacitación y conciencia	Divulgación de información	Impacto en la divulgación de la información del Titular	Debido a falta de capacitación en seguridad, los empleados incumplan con la confidencialidad de la información del Titular pudiendo divulgarla.	5	4	8
			Falta de conciencia acerca de la seguridad	Error en el uso del Reporte Crediticio								
			Trabajo no supervisado del personal externo o de limpieza	Hurto de documentos (Reporte Crediticio)	IDR 21	Actitud deshonesta del personal de limpieza	Divulgación de información y/o robo	Impacto en el cumplimiento de la ley de confidencialidad de la información del Titular	Debido a actitud deshonesta del personal, exista robo de documentación (Reportes) , generandose fuga y atentado contra la confidencialidad del Titular.	5	3	7
A05	Impresora	Organización	Falta o insuficiencia en el acuerdo a nivel de servicio	Incumplimiento en la entrega de servicio de Reporte Crediticio	IDR 22	Falta de mantenimiento del equipo	Falla en el funcionamiento de la Impresora	Impacto en el proceso de Venta de Reporte Crediticio	Impacto en la productividad del negocio	4	2	5
		Hardware	Falta de cuidado y correcto uso por parte del personal no calificado	Mal funcionamiento del equipo								
				Error en el uso								
			Susceptibilidad al polvo, suciedad	Mal funcionamiento del equipo								
				Destrucción del equipo, corrosión								
			Susceptibilidad a altas temperaturas	Mal funcionamiento del equipo								
				Destrucción del equipo, corrosión								
A09	POS	Hardware	Falta de cuidado y correcto uso por parte del personal no calificado	Mal funcionamiento del equipo	IDR 23	Falta de mantenimiento del equipo	Falla en el funcionamiento del POS	Pérdidas financieras	Debido a fallas en el POS no se pueda concretar la venta y haya pérdidas financieras	4	1	4
				Error en el uso								
			Susceptibilidad al polvo, suciedad	Destrucción del equipo, corrosión								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A07	Aplicación Ventas	Software	Gestión deficiente de las contraseñas	Falsificación de derechos	IDR 24	Inadecuadas políticas de almacenamiento de passwords	Contraseñas accesadas por personal no autorizado	Pérdidas financieras y fuga de información	Debido a inadecuadas políticas de almacenamiento de passwords, las contraseñas al Módulo de Ventas sean accesadas por personal no autorizado, pudiendo provocar fuga de información y grandes pérdidas financieras	5	3	7
			Falta de control eficaz del cambio	Mal funcionamiento del software	IDR 25	Mal funcionamiento	Operativa impactada de los procesos de negocio	Impacto en productividad del negocio	Por falta de respaldo o un control eficaz del software, se afecte la operativa de los procesos de negocio soportados y por ende la productividad del negocio.	4	3	6
			Falta de copias de respaldo	Manipulación del software								
		Organización	Falta de procedimiento formal para el registro, retiro del registro de usuario o desbloqueo	Abuso de los derechos	IDR 26	Incumplimiento del procedimiento	Desbloqueo de un usuario de forma constante	Bloqueo reiteraivo y/o ataque mayor	Debido al incumplimiento del procedimiento, se desbloquee un usuario de forma constante sin validar que este sea victima de un ataque externo o interno, se genere un bloqueo reiterativo de usuario y/o ataque mayor.	4	2	5
A10	Manual de Uso de Aplicación Web del Reporte Crediticio	Organización	Falta de políticas para la utilización de activos de la empresa	Error en el uso	IDR 27	Fallas en la gestión de la documentación	Información no disponible	Copia no autorizada / Divulgación de la información	Por fallas en la gestión (almacenamiento) de la documentación (manuales, procedimientos, reporte de turnos e indicadores de gestión), esta no se encuentre disponible o pueda ser accedido por personal no autorizado, facilitando su copia a hurto	4	4	7
				Hurto del manual o copias ilegales								
			Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Copiado del software o el manual								
A12	Cámaras de vigilancia	Hardware	Susceptibilidad al polvo, suciedad	Mal funcionamiento del equipo	IDR 28	Insuficientes politicas de proteccion	Equipos desprotegidos/ Robo	Pérdida de la Confidencialidad de la información del Titular	Debido a insuficientes políticas de protección, cámaras se encuentren desprotegidos y atacantes externos aprovechen vulnerabilidades.	3	2	4
				Destrucción del equipo, corrosión								
			Susceptibilidad a la temperatura	Mal funcionamiento del equipo								
				Destrucción del equipo, corrosión								
A14	Antivirus	Software	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Mal funcionamiento del software	IDR 29	Virus y/o Ataque informático	Bloqueo masivo de cuentas	Indisponibilidad de usuarios y/o aplicaciones	Debido al uso de un software pirata, un virus y/o ataque informático genere bloqueo masivo de cuentas, generando indisponibilidad de usuarios y/o aplicaciones y pérdidas financieras	5	2	6
				Falsificación de derechos								
				Uso de software falso o copiado								
				Abuso de derechos								
			Falta de políticas de seguridad de Firewalls	Uso no autorizado del equipo	IDR 30	No existan políticas de seguridad en Firewalls	Se aperturen puertos incorrectos	Ataques informáticos / Pérdidas financieras / Pérdida de Reputación de la Empresa	Debido a que no se tengan establecidas políticas de Seguridad para accesos a la red a través de Firewalls, se aperturen puertos abriendo nuevas vulnerabilidades y posibilidades de ataque informático.	5	3	7
				Abuso de derechos	IDR 31	Incumplimiento de norma de identificación de usuarios / logs insuficientes	Imposibilidad de identificar a usuario	No sea posible tomar acción correctiva	Debido a incumplimiento de políticas de seguridad de firewall, se instale un equipo Firewall sin proteccion, exponiendo a ataques a los servidores.	5	4	8

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A15	Plataforma	Software	Software pirata	Mal funcionamiento del software	IDR32	Software pirata	Imposibilidad de realizar las labores	Pérdidas financieras	Debido a falta de actualizaciones por ser un software pirata o siplemente por falta de conocimiento de personal no funcionen las aplicaciones generando improductividad en el negocio.	5	1	5
				Falsificación de derechos								
				Abuso de derechos								
			Distribución errada de los derechos de acceso	Abuso de los derechos								
			Defectos bien conocidos en el software									
A16	Base de Datos	Software	Falta o insuficiencia de la prueba del software	Abuso de los derechos	IDR33	Falta de logs	Intentos de acceso no autorizados	Ataques informáticos	Debido a insuficientes logs de auditoría, los intentos no autorizados de acceso a la Base de Datos no sean detectados y se produzcan ataques informáticos.	5	2	6
			Defectos bien conocidos en el software									
			Falta de pruebas de auditoría									
			Distribución errada de los derechos de acceso									
A40	Personal Contabilidad	Personal	Procedimientos inadecuados de contratación	Destrucción de equipos o medios	IDR34	Personal de la Central de Riesgo desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a que el personal desconozca las normas, políticas y criterios de seguridad de información, y en algunos casos debido a procedimientos inadecuados de contratación, se incumplan las normas internas pudiendo generar debilidades y vulnerabilidades de seguridad, errores en el uso de aplicativos y pérdida de integridad de la información	5	3	7
			Uso incorrecto de software y hardware	Error en el uso								
			Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos								
			Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo								
A13	Personal de soporte	Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal	IDR35	Actitud deshonesta del personal	Accesos no autorizados	Pérdidas financieras	Debido a actitud deshonesta del personal, exista fraude interno generándose fuga y/o robo de información.	4	4	7
			Falta de conciencia acerca de la seguridad	Error en el uso								
			Falta de políticas para el uso de correo electrónico	Uso no autorizado del equipo								
			Falta de procedimiento de monitoreo de los recursos de procesamiento información	Abuso de los derechos								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A13	Personal de soporte	Organización	Falta de disposiciones (con respecto a la seguridad) en los contratos con terceros	Abuso de los derechos	IDR36	Incumplimiento de procedimientos	Ataques informaticos a aplicaciones del negocio	Indisponibilidad y/o falta de integridad de las aplicaciones	Por incumplimiento de procedimientos, se produzcan ataques informáticos a aplicaciones del negocio, pudiendo provocar indisponibilidad y/o falta de integridad de las aplicaciones.	5	4	8
			Falta de procedimiento de monitoreo de los recursos de procesamiento información	Abuso de los derechos								
			Falta de reportes sobre fallas incluidos en los registros de administradores y operador	Abuso de los derechos								
			Falta de procedimientos para la introducción del software en los sistemas operativos	Error en el uso	IDR37	Falta de políticas y procedimientos para el personal de soporte	Instalación de aplicativos no autorizados	Ataques informáticos	Instalación de aplicativos de fuente desconocida pudiendo conllevar a ataques informáticos y causando desprestigio a la empresa por la divulgación de la información	5	4	8
A37	Oficina Agencia	Lugar	Uso inadecuado o descuidado del control de acceso físico	Destrucción de equipo o medios	IDR38	Falta de vigilancia	Robo	Pérdida de confidencialidad y financiera	Debido a la falta de seguridad y vigilancia en la entrada de la Agencia pueda efectuarse un robo, daño de equipos o de información afectando la confidencialidad del Titular y pérdidas financieras para la Organización	5	2	6
			Falta de protección física de las puertas y ventanas de la edificación	Hurto de equipo								
A39	Personal de Mantenimiento	Organización	Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos conterceras partes	Abuso de los derechos	IDR39	Personal desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a que el personal de limpieza de la Central desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	5	4	8
			Falta o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos	IDR40							
			Entrenamiento insuficiente en seguridad	Error en el uso	IDR41							
			Trabajo no supervisado del personal de limpieza	Hurto de medios o documentos	IDR42	Inadecuados procedimientos de custodia	Acceso a personal no autorizado a equipos criticos	Indisponibilidad y/o falta de integridad de información	Debido a inadecuados procedimientos de custodia, personal de limpieza tenga acceso a equipos que almacenan o procesan información crítica para el negocio del Banco, pudiendo afectar la disponibilidad e integridad de la información.	5	3	7

2. Matriz de Riesgos: Venta por Web

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A17	Portal Web	Software	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo Distribución errada de los derechos de acceso	Abuso de los derechos	IDR43	Fallas en el Sistema	Ingreso no Autorizado	Pérdida en la integridad de la Información	Personas no autorizadas ingresen al Portal, manipulándolo y causando pérdidas en la integridad de la información	5	2	6
			Interfaz de usuario complicada	Error en el uso	IDR44	Errores en la asignación de perfiles	Inadecuada segregación de funciones	Controles sin efectividad	Debido a errores en la asignación de perfiles definidos para los roles del personal por tener una interfaz complicada para el Portal Web, no exista una adecuada segregación de funciones para los procesos de negocio, por lo que los controles de los procesos pierdan efectividad.	5	3	7
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario Gestión deficiente de las contraseñas	Falsificación de derechos	IDR45	Inadecuadas políticas de almacenamiento de passwords	Contraseñas maestras accesadas por personal no autorizado	Inadecuados niveles de servicio y/o fuga de información	Debido a inadecuadas políticas de almacenamiento de passwords, las contraseñassean accesadas por personal no autorizado, pudiendo afectar los niveles de servicio y/o provocar fuga de información.	5	3	7
			Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR46	Actitud deshonesta del personal y/o falta de procedimiento de baja de usuarios	Accesos a usuarios no autorizados	Robo y/o fuga de información	Debido a actitud deshonesta del personal, exista fraude interno al no realizar las bajas o cambios de roles oportunamente, generandose fuga y/o robo de información. O por no seguir un procedimiento formal se bloqueen los accesos a un usuario que cambia de puesto de trabajo.	5	3	7
A16	Base de Datos	Software	Falta o insuficiencia de la prueba del software Defectos bien conocidos en el software Falta de pruebas de auditoría Distribución errada de los derechos de acceso	Abuso de los derechos	IDR47	Falta de logs	Intentos de acceso no autorizados	Ataques informáticos, pérdida financiera	Debido a insuficientes logs de auditoría, los intentos no autorizados de acceso a la Base de Datos no sean detectados y se produzcan ataques informáticos.	5	2	6

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A28	Servidores de Base de Datos	Hardware	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información	IDR48	Falta de mantenimiento	Acceso a la BD interrumpido	Operativa impactada de los procesos de negocio, improductividad/ Pérdidas financieras	Debido a la falta de mantenimiento, el acceso a la Base de Datos se vea interrumpido	5	2	6
			Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento								
			Almacenamiento sin protección	Hurto de información	IDR49	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a Servidores que almacenan o procesan información crítica para el negocio de la Central, pudiendo afectar la integridad y/o disponibilidad de la información.	5	2	6
			Uso inadecuado o descuidado del control de acceso físico a las edificaciones	Destrucción de equipo o medios								
			Copia no controlada	Hurto de información	IDR50	Inadecuado procedimiento de custodia de información confidencial	Acceso no autorizado a la Base de Datos	Acceso y/o divulgación de información confidencial	Debido a inadecuado procedimiento de custodia de información confidencial, la Base de datos sea accesada por personal no autorizado con posible riesgo de acceso y/o divulgación de información.	5	3	7
		Lugar	Falta de protección física de las puertas y ventanas de la edificación	Hurto de Servidor	IDR51	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio de la Central como los Servidores, pudiendo afectar la integridad y/o disponibilidad de la información.	5	3	7
			Ubicación en un área susceptible de inundación	Inundación								
A19	Correo electrónico	Personal	Falta de políticas para el uso del correo electrónico	Uso no autorizado del equipo	IDR52	Personal de la Central de Riesgo desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a que el personal de la Central de Riesgo desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internas relacionadas con el uso de correo electrónico pudiendo generar debilidades y vulnerabilidades de seguridad.	5	3	7
			Entrenamiento insuficiente en seguridad	Error en el uso								
		Organización	Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Abuso de los derechos	IDR53	Inadecuado procedimiento de contratación y disposiciones en contrato	Incorrecto uso de correo electrónico	Vulnerabilidad de seguridad	Debido a un inadecuado procedimiento de contratación como la evidencia de antecedentes penales y policiales, desarrollo de pruebas de competencia, desconocimiento de las normas, políticas y criterios de seguridad de información y falta de disposiciones en contratos se incumplan las normas internas pudiendo generar debilidades y vulnerabilidades en la seguridad de la Central de Riesgo.	5	4	8
			Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Falsificación y Abuso de derechos	IDR54	Falta de procesos disciplinarios	Ataques informáticos	Pérdida en la integridad de la Información, Robo / divulgación de la información	Debido a la falta de procesos disciplinarios en caso de incidentes de seguridad a través del uso del correo electrónico no sea posible tomar acciones correctivas.	5	3	7

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A02	Aplicación Web Reporte Crediticio Online	Software	El aplicativo web contiene defectos o fallas en su desarrollo.	Mal funcionamiento del software	IDR57	Inadecuados procesos de detección	Intentos no autorizados de acceso a información	Debido al Robo o fuga de información haya pérdidas financieras	Debido a un mal funcionamiento del aplicativo web podrían haber intentos no autorizados de acceso que no sean detectados y se produzcan ataques informáticos, lo que conlleva a robo o fuga de información	5	3	7
				Abuso de derechos		Fallas en el aplicativo Web	Falla en los accesos	Imposibilidad de ejecutar labores	Debido a fallas en aplicativo web (por ejm: el personal podría no contar con accesos disponibles) se imposibiliten las labores cotidianas trayendo pérdidas financieras para la empresa e improductividad	4	2	5
			Falta de terminación de Sesión cuando se cierra el aplicativo.	Falsificación de derechos	IDR58	Fallas en el aplicativo Web	Usuarios no autorizados ingresen al sistema	Falta de integridad y/o disponibilidad de la información	Debido a fallas de terminación de sesión del aplicativo Web, usuarios a quienes no le corresponden acceso, ingresen al sistema pudiendo afectar la integridad y/o disponibilidad de la información.	5	1	5
				Abuso de derechos								
			Falta de mecanismos de autenticación e identificación de usuario	Falsificación de derechos	IDR59	Falta de identificación de usuarios / logs insuficientes	Imposibilidad de identificar a usuario	No sea posible tomar acción correctiva	Debido a la falta de mecanismos de autenticación e identificación de usuarios / logs insuficientes, no sea posible identificar a usuario y por ende no sea posible tomar acción correctiva.	5	2	6
			Interfaz de usuario complicada	Error en el uso	IDR60	Interfaz compleja	Error en el uso del aplicativo	Fuga y/o divulgación de la información	Debido a una interfaz complicada , no se realice correctamente la definición de los perfiles de accesos y por ende los usuarios tengan accesos de más o restringidos.	4	3	6
			Faltas de las pruebas de software	Abuso de derechos	IDR61	Inadecuada gestión de accesos	Usuarios con mas accesos de los definidos inicialmente	Impacto en productividad del negocio	Debido a la falta de pruebas en el software traiga como consecuencia una inadecuada gestión de accesos y se otorguen mayores accesos a los usuarios de los que se definieron inicialmente, posibilitando el uso incorrecto de los mismos.	4	3	6
			Falta de documentación y actualización de dicha documentación	Error en el uso	IDR62	Fallas en la gestión de la documentación	Información no disponible	Pérdida de Integridad en la información, fuga de información, divulgación	Por falta de documentación (manuales, procedimientos, reporte de turnos e indicadores de gestión), haya la posibilidad de fallas en el otorgamiento de accesos generando fuga de información	4	4	7
			Gestión deficiente de las contraseñas	Falsificación de derechos	IDR63	Inadecuadas políticas de almacenamiento de passwords	Contraseñas maestras accesadas por personal no autorizado	Inadecuados niveles de servicio y/o fuga de información	Debido a inadecuadas políticas de almacenamiento de passwords, las contraseñas maestras sean accesadas por personal no autorizado, pudiendo afectar los niveles de servicio y/o provocar fuga de información.	5	4	8

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A02	Aplicación Web Reporte Crediticio Online	Software	Falta de control eficaz del cambio	Mal funcionamiento del aplicativo	IDR64	Errores en la asignación de perfiles	Inadecuada segregación de funciones	Controles sin efectividad	Debido a un ineficiente control de cambios del aplicativo exista errores en la asignación de perfiles definidos para los roles del personal y por consiguiente no exista una adecuada segregación de funciones para los procesos de negocios de la Central de Riesgo, por lo que los controles de los procesos pierdan efectividad.	4	2	5
			Descargas y usos no controlados del aplicativo	Manipulación incorrecta del aplicativo	IDR65	Falta de políticas de seguridad y determinación de owners	Acceso al aplicativo de usuarios no autorizados	Divulgación de información	Debido a que no exista una relación de aplicativos (cliente/servidor y host) vs. owners, se otorguen o eliminen accesos sin contar con todas las aprobaciones requeridas, pudiendo facilitar la manipulación del aplicativo y la divulgación de información.			
			Falta de protección física en las puertas y ventanas de la Agencia o edificación	Hurto	IDR66	Falta de protección física	Robo	Pérdidas financieras	Debido a la falta de protección física en las puertas se produzca robo de información, fuga o divulgación lo que conlleve a pérdidas financieras	5	1	5
		Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de derechos	IDR67	Errores en la baja de usuarios	Accesos a usuarios no autorizados	Robo y/o fuga de información	Debido a errores en el procedimiento de baja de usuarios, no se dé de baja o bloquee los accesos a un usuario que cambia de puesto de trabajo, posibilitando el robo y/o fuga de información.	5	4	8
A40	Personal Contabilidad	Personal	Procedimientos inadecuados de contratación	Destrucción de equipos o medios	IDR68	Personal de Contabilidad desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a que el personal desconozca las normas, políticas y criterios de seguridad de información, y en algunos casos debido a procedimientos inadecuados de contratación, se incumplan las normas internas pudiendo generar debilidades y vulnerabilidades de seguridad, errores en el uso de aplicativos y pérdida de integridad de la información	5	3	7
			Uso incorrecto de software y hardware	Error en el uso								
			Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos								
			Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A13	Personal de soporte	Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal	IDR69	Personal desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a que el personal desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	4	4	7
			Falta de conciencia acerca de la seguridad	Error en el uso								
			Falta de políticas para el uso de correo electrónico	Uso no autorizado del equipo	IDR70	Falta de políticas sobre el uso de correo electrónico	Ataques informáticos	Incumplimiento de la ley	Por falta de políticas para el uso del correo electrónico, se generen debilidades y vulnerabilidades de seguridad (ataques informáticos) y se divulgue información o se pierda la integridad de la misma	5	4	8
		Organización	Falta de disposiciones (con respecto a la seguridad) en los contratos con terceros	Abuso de los derechos	IDR71	Actitud deshonesta del personal y falta de disposiciones en contratos	Fuga y/o robo de información	Pérdidas financieras / Incumplimiento de la ley	Debido a la falta de disposiciones en los contratos y a una actitud deshonesta del personal, exista fraude interno, generandose fuga y/o robo de información.	5	4	8
			Falta de proceso formal para la revisión (supervisión) de los derechos de acceso		IDR72	Falta de proceso formal de revisión de accesos	Usuarios se les otorgue accesos que no le corresponden	Vulnerabilidad de seguridad	Debido a la falta de un proceso formal para la revisión de los accesos del personal de soporte a información confidencial, se les otorgue accesos privilegiados, posibilitando el inadecuado uso y la pérdida de confidencialidad e integridad de la información	5	4	8
			Falta de procedimientos para la introducción del software en los sistemas operativos	Error en el uso	IDR73	Falta de procedimientos para la introducción de sw	Fuga y/o robo de información	Pérdidas financieras / Incumplimiento de la ley	Debido a la falta de procedimientos para la introducción de sw y una actitud deshonesta del personal, exista fraude interno, generandose fuga y/o robo de información.	5	4	8

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A51	Personal de Tecnología de Información	Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal	IDR74	Personal desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a que el personal desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	5	4	8
			Procedimientos inadecuados de contratación	Destrucción de equipos o medios								
			Entrenamiento insuficiente en seguridad	Error en el uso								
			Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos	IDR75	Falta de mecanismos de monitoreo	Se otorguen o eliminen accesos sin aprobaciones	Divulgación de información	Debido a que no se encuentre actualizada la relación de aplicativos (cliente/servidor y host) vs. owners, se otorguen o eliminen accesos a empleados de TI sin contar con todas las aprobaciones requeridas, pudiendo facilitar la divulgación de información.	5	4	8
			Trabajo no supervisado	Hurto de información o medios	IDR76	Fallas en la gestión de accesos al Personal de TI	Personas no autorizadas con accesos generándose fuga y/o robo de información	Incumplimiento de la ley - pérdidas financieras	Debido a la falta de supervisión del personal de TI, personas a las que no corresponde cuenten con accesos a los que ya no están autorizados, pudiendo generarse fuga y/o robo de información.	5	4	8
		Lugar	Falta de protección física de las puertas	Hurto de equipo	IDR77	Insuficientes politicas de proteccion	Robo de equipo	Atacantes externos aprovechen vulnerabilidades, divulgación de información	Debido a insuficientes políticas de protección, los equipos se encuentren desprotegidos y atacantes externos aprovechen vulnerabilidades.	5	4	8
		Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR78	Incumplimiento de procedimientos	Ataques informaticos a aplicaciones del negocio	Indisponibilidad y/o falta de integridad de las aplicaciones	Por incumplimiento de procedimientos, se produzcan ataques informáticos a aplicaciones del negocio, pudiendo provocar indisponibilidad y/o falta de integridad de las aplicaciones.	5	4	8
			Falta de proceso formal para la revisión (supervisión) de los derechos de acceso									
			Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con terceros									
			Falta o insuficiencia en el acuerdo a nivel de servicio (terceros)	Incumplimiento en el mantenimiento del sistema de información	IDR79	Actitud deshonesta del personal	Robo o alteración de información	Incumplimiento de ley	Por falta de disposiciones en contratos, personal deshonesto que tenga acceso a equipos o aplicativos que poseen información crítica para el negocio del Banco, pudiendo afectar la integridad y/o disponibilidad de la información.	5	5	9

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A20	Servidor de Correo	Hardware	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información	IDR55	Falta de mantenimiento	Acceso a la BD interrumpido	Operativa impactada de los procesos de negocio, improductivadad/ Pérdidas financieras	Debido a la falta de mantenimiento, el envío de correos electrónicos se vea interrumpido	5	3	7
			Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento								
			Almacenamiento sin protección	Hurto de información	IDR56	Inadecuado procedimiento de custodia de equipos y como consecuencia de información confidencial	Información confidencial accesada por personal no autorizado	Acceso y/o divulgación de información confidencial	Debido a inadecuados procedimientos de custodia y falta de procedimientos para copias, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio, pudiendo afectar la disponibilidad e integridad de la información.	5	3	7
			Copia no controlada	Hurto de información								
		Lugar	Falta de protección física de las puertas y ventanas de la edificación	Hurto de Servidor								

3. Matriz de Riesgos: Generar Venta Servicios Complementarios

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A22	Equipo Telefónico	Red	Líneas de comunicación sin protección Tráfico sensible sin protección	Escucha subrepticia	IDR198	Líneas sin protección	divulgación de la información	Incumplimiento de la ley	Divulgación de la información relacionada con el servicio brindado y como consecuencia pérdida de la confidencialidad	5	2	6
		Personal	Falta de políticas para el uso correcto del equipo	Uso no autorizado del equipo	IDR199	Insuficientes politicas de proteccion	Equipos desprotegidos	Atacantes externos aprovechen vulnerabilidades	Debido a insuficientes políticas de protección, los equipos telefónicos se encuentren desprotegidos y atacantes externos aprovechen vulnerabilidades.	4	1	4
A23	Personal Comercial - Ventas	Personal	Procedimientos inadecuados de contratación	Error en el uso de aplicativos Destrucción de equipos Procesamiento ilegal de los datos	IDR200	Incumplimiento de procedimientos	Ataques informaticos a aplicaciones del negocio	Indisponibilidad y/o falta de integridad de las aplicaciones	Por incumplimiento de procedimientos, se produzcan ataques informáticos a aplicaciones del negocio, o a equipos como servidores pudiendo provocar indisponibilidad y/o falta de integridad de las aplicaciones e información de Titulares	5	4	8
		Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario Falta de proceso formal para la revisión (supervisión) de los derechos de acceso Falta de procedimiento de monitoreo de los recursos de procesamiento información	Abuso de los derechos	IDR201	Inadecuado procedimiento de baja de accesos	Falta de accesos	Improductividad	Debido a inadecuado procedimiento de baja de accesos, personal no pueda realizar sus labores por la falta de accesos a los diferentes sistemas, generando improductividad.	5	4	8
			Falta de políticas sobre el uso del correo electrónico	Error en el uso	IDR202	Falta de políticas sobre el uso de correo electrónico	Ataques informáticos	Incumplimiento de la ley	Por falta de políticas para el uso del correo electrónico, se generen debilidades y vulnerabilidades de seguridad (ataques informáticos) y se divulgue información o se pierda la integridad de la misma	5	3	7
			Falta de procedimientos para la introducción del software en los sistemas operativos		IDR203	Falta de procedimientos para la introducción de sw	Fuga y/o robo de información	Pérdidas financieras / Incumplimiento de la ley	Debido a la falta de procedimientos para la introducción de sw y una actitud deshonesta del personal de ventas, exista fraude interno, generandose fuga y/o robo de información.	5	3	7

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A19	Correo electrónico	Personal	Falta de políticas para el uso del correo electrónico	Uso no autorizado del correo eletrónico	IDR204	Personal de la Central de Riesgo desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a que el personal de la Central de Riesgo desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internas relacionadas con el uso de correo electrónico pudiendo generar debilidades y vulnerabilidades de seguridad.	5	3	7
			Entrenamiento insuficiente en seguridad	Error en el uso								
		Organización	Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Abuso de los derechos	IDR205	Inadecuado procedimiento de contratación y disposiciones en contrato	Incorrecto uso de correo electrónico	Vulnerabilidad de seguridad	Debido a un inadecuado procedimiento de contratación como la evidencia de antecedentes penales y policiales, desarrollo de pruebas de competencia, desconocimiento de las normas, políticas y criterios de seguridad de información y falta de disposiciones en contratos se incumplan las normas internas pudiendo generar debilidades y vulnerabilidades en la seguridad de la Central de Riesgo.	5	4	8
			Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Falsificación y Abuso de derechos	IDR206	Falta de procesos disciplinarios	Ataques informáticos	Pérdida en la integridad de la Información, Robo / divulgación de la información	Debido a la falta de procesos disciplinarios en caso de incidentes de seguridad a través del uso del correo electrónico no sea posible tomar acciones correctivas.	5	3	7
A20	Servidor de Correo	Hardware	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información	IDR207	Falta de mantenimiento	Acceso a la BD interrumpido	Operativa impactada de los procesos de negocio, improductivada d/ Pérdidas financieras	Debido a la falta de mantenimiento, el acceso a la Base de Datos se vea interrumpido	5	5	9
			Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento								
			Almacenamiento sin protección	Hurto de información	IDR208	Inadecuado procedimiento de custodia de equipos y como consecuencia de información confidencial	Información confidencial accesada por personal no autorizado	Acceso y/o divulgación de información confidencial	Debido a inadecuados procedimientos de custodia y falta de procedimientos para copias, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio, pudiendo afectar la disponibilidad e integridad de la información.	5	4	8
			Copia no controlada	Hurto de información								
		Lugar	Falta de protección física de las puertas y ventanas de la edificación	Hurto de Servidor								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A24	CD encriptado	Hardware	Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del CD Polvo, corrosión	IDR209	Inadecuadas políticas de almacenamiento	Información no disponible	Impacto en productividad del negocio, incumplimiento de contrato, incumplimiento de la ley	Por inadecuadas políticas de almacenamiento, se dañen CDs que almacenan información crítica para el negocio de la Central, pudiendo afectar la integridad y/o disponibilidad de la información.	5	2	6
			Almacenamiento sin protección	Hurto o destrucción de CD	IDR210	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a los Cds que almacenan información crítica para el negocio de la Central de Riesgo, pudiendo afectar la integridad y/o disponibilidad de la información o Robo	5	3	7
			Copia no controlada									
		Personal	Trabajo no supervisado del personal externo o de limpieza									
A26	Operadores	Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal	IDR211	Falta de disponibilidad de operadores	Operativa impactada de los procesos de negocio	Impacto en productividad del negocio	Debido a la falta de disponibilidad de operadores, haya un grave impacto en la productividad del negocio	5	4	8
			Procedimientos inadecuados de contratación	Destrucción de equipos o medios	IDR212	Desconocimiento de operadores de las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a que el personal desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	5	5	9
			Entrenamiento insuficiente en seguridad	Error en el uso de aplicaciones								
			Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos	IDR213	Falta de mecanismos de monitoreo	Se otorguen o eliminen accesos sin aprobaciones	Divulgación de información y/o pérdida de integridad	Debido a que no se cuente con una relación de aplicativos (cliente/servidor y host) vs. owners, se otorguen o eliminen accesos a operadores sin contar con todas las aprobaciones requeridas, pudiendo facilitar la divulgación de información y/o pérdida de integridad de la información	5	4	8
			Trabajo no supervisado del personal	Hurto de medios o documentos	IDR214	Fallas en la gestión de accesos a personal	Personas no autorizadas con accesos generándose fuga y/o robo de información	Incumplimiento de la ley - pérdidas financieras	Debido a la falta de supervisión del personal, personas a las que no corresponde cuenten con accesos a los que ya no están autorizados, pudiendo generarse fuga y/o robo de información.	5	4	8
		Organización	Falta de reportes sobre fallas incluidos en los registros de operadores	Abuso de los derechos	IDR215	Falta de registro de bitácoras e incidentes en seguridad	Operativa impactada de los procesos de negocio	Impacto en productividad del negocio	Debido a falta de procedimientos de registros de bitácora, no se puedan tomar acciones correctivas por tanto no se registren acciones correctivas alrededor de los incidentes en las actividades diarias	4	3	6
			Falta de registros en las bitácoras *(logs)	Error en el uso								
			Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos	IDR216	Actitud deshonesta del personal y falta de disposiciones en contratos	Fuga y/o robo de información	Pérdidas financieras / Incumplimiento de la ley	Debido a la falta de disposiciones en los contratos y a una actitud deshonesta del personal, exista fraude interno, generandose fuga y/o robo de información o pérdida de su integridad	5	5	9

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A27	Documento Excel con el registro de los Servicios (Macro)	Personal	Trabajo no supervisado del personal externo o de limpieza	Hurto de documento	IDR217	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Pérdidas finacieras	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a información confidencial, divulgándola a la competencia por ejemplo.	5	4	8
		Organización	Falta o insuficiencia de políticas sobre limpieza de escritorio y de pantalla	Uso no autorizado del equipo	IDR218	Falta de políticas sobre limpieza de escritorio	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a la falta de políticas internas, personal no autorizado acceda a iinformación crítica (personal de limpieza)	5	4	8
			Falta de control eficaz del cambio y protección de documento	Mal funcionamiento / acceso no autorizado	IDR219	Actitud del personal	Acceso no autorizado	Fuga y/o robo de información generando pérdidas financieras	Personal de actitud deshonesta acceda al documento, o personal no autorizado logre acceder por un mal funcionamiento, generándose pérdida de la intgegridad o robo de información	5	4	8
A28	Servidores de Base de Datos	Hardware	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información	IDR220	Falta de mantenimiento	Acceso a la BD interrumpido	Operativa impactada de los procesos de negocio, improductivadad/ Pérdidas financieras	Debido a la falta de mantenimiento, el acceso a la Base de Datos se vea interrumpido	5	3	7
			Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento								
			Almacenamiento sin protección	Hurto de información	IDR221	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso (por ejem: fallas en custodia de archivos que contiene los passwords de los usuarios genéricos de aplicación del ambiente de producción,) personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio, pudiendo afectar la integridad y/o disponibilidad de la información.	5	4	8
			Uso inadecuado o descuidado del control de acceso físico a las edificaciones	Destrucción de equipo o medios								
			Copia no controlada	Hurto de información								
		Lugar	Falta de protección física de las puertas y ventanas de la edificación	Hurto de Servidor	IDR222	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio de la Central como los Servidores, pudiendo afectar la integridad y/o disponibilidad de la información.	5	2	6

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A29	Servidores de Archivos	Hardware	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información	IDR223	Falta de mantenimiento	Acceso a la BD interrumpido	Operativa impactada de los procesos de negocio, improductivadad/ Pérdidas financieras	Debido a la falta de mantenimiento, el acceso a la Base de Datos se vea interrumpido	5	2	6
			Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento								
			Almacenamiento sin protección	Hurto de información	IDR224	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso personal no autorizado tenga acceso a servidores de archivos que contienen nformación crítica para el negocio, pudiendo afectar la integridad y/o disponibilidad de la información.	4	3	6
			Copia no controlada	Hurto de información								
		Lugar	Falta de protección física de las puertas y ventanas de la edificación	Hurto de Servidor	IDR225	Inadecuados procedimientos de custodia	Acceso a personal no autorizado a equipos criticos	Indisponibilidad y/o falta de integridad de información	Debido a inadecuados procedimientos de custodia, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio de la Central, pudiendo afectar la disponibilidad e integridad de la información.	5	3	7
		Organización	Falta de autorización de los recursos de procesamiento de la información									
A30	Intranet de la Central de Riesgo	Software	Interfaz de usuario complicada	Error en el uso	IDR226	Errores en la asignación de perfiles	Inadecuada segregación de funciones	Controles sin efectividad	Debido a una interfaz complicada se realice una errónea asignación de perfiles definidos para los roles del personal.	4	2	5
			Falta de documentación y actualización de dicha documentación		IDR227	Fallas en la gestión de la documentación	Información no disponible	Pérdida de Integridad en la información, fuga de información, divulgación	Por falta de documentación (manuales, procedimientos, reporte de turnos e indicadores de gestión), haya la posibilidad de fallas en el otorgamiento de accesos generando fuga de información	4	4	7
			Falta de mecanismos de identificación y autentificación	Falsificación de derechos	IDR228	Incumplimiento de norma de identificación de usuarios y/o procedimiento de elaboración de reporte	Falta de identificación de usuarios que realizo uso inadecuado de accesos	Dificultad para tomar acciones correctivas	Por incumplimiento de norma de identificación de usuarios y/o procedimiento de elaboración de reporte, no sea posible identificar a usuario que realizó uso inadecuado de accesos y se dificulten las acciones correctivas.	5	4	8
			Gestión deficiente de las contraseñas		IDR229	Inadecuada política de otorgamiento de accesos	accesos de los usuarios que se encuentren de vacaciones no sean deshabilitados	Fuga y/o robo de información	Debido a inadecuada poítica de otorgamiento de accesos, los accesos de los usuarios que se encuentren de vacaciones no sean deshabilitados durante ese período, pudiendo ser vulnerados por un tercero.	4	4	7
		Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A31	Medios de Almacenamiento	Hardware	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información	IDR230	Falta de mantenimiento	Pérdida de información	Operativa impactada de los procesos de negocio, improductivadad/ Pérdidas financieras	Debido a la falta de mantenimiento, el acceso a la Base de Datos se vea interrumpido	5	2	6
			Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento								
			Almacenamiento sin protección	Hurto de medios	IDR231	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso personal no autorizado tenga acceso a servidores de archivos que contienen nformación crítica para el negocio, pudiendo afectar la integridad y/o disponibilidad de la información.	5	3	7
			Copia no controlada									
			Falta de conciencia acerca de la seguridad	Error en el uso	IDR232	Personal desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a que el personal desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	5	3	7
		Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios	IDR233	Inadecuada gestión de accesos	Personal no autorizado acceda al centro de operaciones	Daño a equipos y/o robo de información	Debido a una inadecuada gestión de los accesos , personal no autorizado pueda acceder al centro de operaciones, pudiendo provocar daños a equipos y robo de medios de almacenamiento	4	4	7
		Organización	Falta de protección física de las puertas y ventanas de la edificación	Hurto de Medios de Almacenamiento								
			Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con terceras partes	Abuso de los derechos	IDR234	Actitud deshonesta del personal y falta de disposiciones en contratos	robo de información	Pérdidas financieras / Incumplimiento de la ley	Debido a la falta de disposiciones en los contratos y a una actitud deshonesta del personal, exista fraude interno, generandose robo de información.	5	4	8
			Falta de autorización de los recursos	Hurto de medios	IDR235	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso (por ejem: fallas en custodia de los medios de almacenamiento) personal no autorizado tenga acceso a medios que almacenan información crítica para el negocio de la Central, pudiendo afectar la integridad y/o disponibilidad de la información.	5	3	7

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A33	Microsoft Office 2007 - Excel 2007	Software	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Mal funcionamiento de sw	IDR236	sw pirata	Imposibilidad de realizar las labores	Pérdidas financieras	Debido al mal funcionamiento del sw, no se puedan realizar las actividades diarias (p.e. elaboraciones de reportes) generando improductividad en el negocio.	5	2	6
A34	Infraestructura de red	Red	Falta de prueba del envío o la recepción de mensajes	Negación de acciones	IDR237	falta de pruebas	Imposibilidad de realizar las labores cotidiananas	impacto en productividad	Debido a la falta de pruebas, personal no pueda realizar el envío de mensajes imposibilitando sus labores cotidianas y la entrega de servicios afectando la operabilidad y productividad del negocio	5	2	6
			Tráfico sensible sin protección	Saturación del sistema de información	IDR238	Inadecuados procesos de detección y falta de protección de la red	Ataques informáticos	Pérdidas financieras	Debido al tráfico y a inadecuados procesos de detección, los intentos no autorizados de acceso a información de aplicativos no sean detectados y se produzcan ataques informáticos.	5	3	7
			Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones	IDR239	Falta de mantenimiento	Pérdida de conexión	Incumplimiento de contrato / Pérdidas financieras	Debido a la falta de mantenimieniento de la infraestructura, la red no se encuentre disponible imposbilitando la entrega del servicio.	5	2	6
			Arquitectura insegura de la red	Espionaje remoto	IDR240	Falta de adecuadas políticas de protección	Ataques informaticos a aplicaciones del negocio	Incumplimiento de contrato/ Incumplimiento de la ley/ Pérdidas Financieras	Debido a una arquitectura insegura se produzcan ataques informáticos a las principales aplicaciones del negocio , pudiendo incluso provocar indisponibilidad y/o falta de integridad de las aplicaciones.	5	3	7
			Conexiones de red pública sin protección	Uso no autorizado del equipo	IDR241	Insuficientes politicas de proteccion	ataques informáticos	Indisponibilidad de los servicios / Pérdidas financieras	Debido a insuficientes políticas de protección, los equipos se encuentren desprotegidos y atacantes externos aprovechen vulnerabilidades.	5	3	7
A35	Dominio Organizativo	Red	Falta de identificación y autentificación de emisor y receptor	Falsificación de derechos	IDR242	Inadecuados procesos de detección	Intentos no autorizados de acceso a información	Pérdida de la integridad de la información / Robo de información	Debido a una falta de políticas de seguridad para la identificación y autenticación de emisor y receptor e inadecuados procesos de detección, los intentos no autorizados de acceso a información de aplicativos no sean detectados y se produzcan ataques informáticos.	5	3	7
			Transferencia de contraseñas autorizadas	Espionaje remoto	IDR243	Inadecuadas políticas de seguridad	Acceso a información crítica y divulgación	Incumplimiento de la ley / Pérdidas financieras	Divulgación de la información relacionada con el servicio brindado y como consecuencia pérdida de la confidencialidad	5	4	8

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A36	Edificio	Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios	IDR244	Inadecuadas políticas de acceso al edificio	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Debido a inadecuadas políticas de seguridad para el acceso físico al edificio, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio del Banco, pudiendo afectar la integridad y/o disponibilidad de la información.	5	3	7
			Falta de protección física de las puertas y ventanas de la edificación	Hurto de equipo								
			Red energética inestable	Pérdida del suministro de energía	IDR245	Falta de mantenimiento	Indisponibilidad de servicios	Pérdidas financieras / Incumplimiento de la ley / Incumplimiento de contrato	Debido a una falta de mantenimiento de las instalaciones se genera una pérdida del suministro de energía generando indisponibilidad de los servicios.	5	3	7
A38	Impresora Industrial	Organización	Falta o insuficiencia en el acuerdo a nivel de servicio	Incumplimiento en la entrega de servicio de Cartas Cobranza	IDR246	Falta de mantenimiento y/o error en el uso	Imposibilidad de la entrega de servicios	Pérdida financiera	Incumplimiento de contrato e imposibilidad de entrega del servicio, debido al mal fucionamiento de impresora	4	2	5
		Hardware	Falta de cuidado y correcto uso por parte del personal no calificado	Mal funcionamiento del equipo								
				Error en el uso								
			Susceptibilidad al polvo, suciedad	Mal funcionamiento del equipo								
				Destrucción del equipo, corrosión								
			Susceptibilidad a altas temperaturas	Mal funcionamiento del equipo								
				Destrucción del equipo, corrosión								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A39	Personal de Mantenimiento	Organización	Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos conterceras partes	Abuso de los derechos	IDR247	Personal desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a que el personal de limpieza de la Central desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	5	4	8
			Falta o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos								
			Entrenamiento insuficiente en seguridad	Error en el uso								
			Trabajo no supervisado del personal de limpieza	Hurto de medios o documentos	IDR248	Inadecuados procedimientos de custodia	Acceso a personal no autorizado a equipos criticos	Indisponibilidad y/o falta de integridad de información	Debido a inadecuados procedimientos de custodia, personal de limpieza tenga acceso a equipos que almacenan o procesan información crítica para el negocio del Banco, pudiendo afectar la disponibilidad e integridad de la información.	5	3	7
A40	Personal Contabilidad	Personal	Uso incorrecto de software y hardware	Error en el uso	IDR249	Personal no tenga el conocimiento suficinete para implementar y administrar la herramienta	Errores en el uso de aplicativos	Pérdida de integridad de la información	Debido a que personal no tenga el conocimiento suficiente para la utilización de aplicaciones o hw y a falta de monitorio, se presenten errores o ingreso ilegal de data.	4	3	6
			Procedimientos inadecuados de contratación	Destrucción de equipos o medios	IDR250	Personal de Contabilidad desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a que el personal desconozca las normas, políticas y criterios de seguridad de información, y en algunos casos debido a procedimientos inadecuados de contratación, se incumplan las normas internas pudiendo generar debilidades y vulnerabilidades de seguridad, errores en el uso de aplicativos y pérdida de integridad de la información	5	3	7
			Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos								
			Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A51	Personal de Tecnología de Información	Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal	IDR251	Inadecuados procesos de contrtación y falta de capacitación	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información / Pérdidas finacieras /Robo de información	Debido a que el personal desconozca las normas, políticas y criterios de seguridad de información, y en algunos casos debido a procedimientos inadecuados de contratación, se incumplan las normas internas pudiendo generar debilidades y vulnerabilidades de seguridad, errores en el uso de aplicativos, ypérdida de integridad de la información e incluso hurto y fraude.	5	4	8
			Procedimientos inadecuados de contratación	Destrucción de equipos o medios								
			Entrenamiento insuficiente en seguridad	Error en el uso								
			Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos								
			Trabajo no supervisado	Hurto de información o medios								
		Lugar	Falta de protección física de las puertas	Hurto de equipo o información	IDR252	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso físico, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio (medios de almacenamiento) pudiendo afectar la integridad y/o disponibilidad de la información.	5	4	8
		Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR253	Falta de segregación de funciones	Unidad sea responsable de definir/crear/aprobar cambios	Errores y/o abuso de funciones	Debido a falta de segregación de funciones, una misma unidad sea responsable de definir, crear y aprobar cambios en producción relacionado a roles, ocasionando errores y/o abuso de funciones.	5	3	7
			Falta de proceso formal para la revisión (supervisión) de los derechos de acceso									
			Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con terceros									
			Falta o insuficiencia en el acuerdo a nivel de servicio	Incumplimiento en el mantenimiento del sistema de información	IDR254	Falta de mantenimiento	Falla en los aplicativos	Acceso no autorizados, robo de información	Fallas en el funcionamiento de los aplicativos generando vulnerabildiades en la seguridad, accesos no autorizados, robo de información.	5	3	7

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A52	Personal de Tecnología como Servicio	Personal	Entrenamiento insuficiente en seguridad	Hurto de información	IDR255	Personal desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad / Robo de información / Divulgación / Pérdida de Integridad	Debido a que el personal de la Central desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	5	4	8
			Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo								
		Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR256	Falta de designación de owners	Se otorguen o eliminen accesos sin aprobaciones	Divulgación de información / pérdidas financieras	Debido a que no se cuenta con una relación de aplicativos (cliente/servidor y host) vs. owners, se otorguen o eliminen accesos sin contar con todas las aprobaciones requeridas, pudiendo facilitar la divulgación de información y el hurto de Información, ocasionando grandes pérdidas financieras	4	3	6
			Falta de proceso formal para la revisión (supervisión) de los derechos de acceso									
			Falta de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones								
			Falta de políticas sobre el uso del correo electrónico	Error en el uso								
			Falta de procedimientos para la introducción del software en los sistemas operativos									
			Falta de procedimientos para el manejo de información clasificada									
			Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos								
			Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo o información								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A78	Personal Servicio al Cliente	Personal	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo	IDR257	Actitud deshonesta del personal	Accesos inadecuados	Fuga y/o robo de información	Debido a actitud deshonesta del personal, exista fraude interno al no realizar las bajas o cambios de roles oportunamente, generandose fuga y/o robo de información.	5	4	8
			Falta de revisiones de los derechos de acceso	Abuso de los derechos								
A41	Aplicación Web de Seguimiento	Software	Distribución errada de los derechos de acceso	Abuso de los derechos	IDR258	Falta de políticas de otorgamiento de accesos	Indisponibilidad de servicio	Pérdidas financieras	Acceso no autorizado pudiendo generar indisponibilidad del acceso al aplicativo	5	3	7
			Falta de documentación y actualización de dicha documentación	Error en el uso	IDR259	Fallas en la gestión de la documentación	Información no disponible	Pérdida de Integridad en la información, fuga de información, divulgación	Por falta de documentación (manuales, procedimientos, reporte de turnos e indicadores de gestión), haya la posibilidad de fallas en el otorgamiento de accesos generando fuga de información	4	4	7
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos	IDR260	Falta de procedimientos y políticas de seguridad	Ataques informaticos a aplicaciones del negocio	ndisponibilidad y/o falta de integridad de las aplicaciones	Debido a la falta de autentificación personal no autorizado acceda al aplicativo y se produzcan ataques a la aplicación	5	3	7
A63	Sistema de decisiones	Software	Interfase de usuario complicada	Error en el uso	IDR261	Interfaz complicada / Falta de documentacion	Errores en el uso de aplicativos	Acceso no autorizados, robo de información	Debido a la falta de documentacion , halla una una falla en la designación de perfiles y roles y configuración de parámetros pudiendo generar fallas en la entrega del servicio, improductividad y accesos no autorizados.	4	4	7
			Falta de documentación									
			Configuración incorrecta de parámetros									
			Falta de control eficaz del cambio	Mal funcionamiento del software	IDR262	Falla en el funcionamiento	Acceso no autorizado	Ataques informáticos / Pérdidas financieras	Fallas en el funcionamiento de los aplicativos generando vulnerabildiades en la seguridad, accesos no autorizados, robo de información.	5	3	7

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A16	Base de Datos Microsoft Sql Server 2003 - 2008	Software	Falta o insuficiencia de la prueba del software	Abuso de los derechos	IDR263	Falta de logs	Intentos de acceso no autorizados	Ataques informáticos	Debido a insuficientes logs de auditoría, los intentos no autorizados de acceso a la Base de Datos no sean detectados y se produzcan ataques informáticos.	5	4	8
			Defectos bien conocidos en el software									
			Falta de pruebas de auditoría									
			Distribución errada de los derechos de acceso		IDR264	Inadecuado procedimiento de identificación de funciones	Definición incorrecta de perfiles de acceso	Usuarios tengan accesos de más o restringidos	Debido a un inadecuado procedimiento de identificación de funciones, no se realice correctamente la definición de los perfiles de accesos y por ende los usuarios tengan accesos de más o restringidos.	5	4	8
A48	Web Service	Software	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento	IDR265	Falla en el funcionamiento	Falla en los servicios	Pérdidas financieras / Incumplimiento de contrato	Debido al mal funcionamiento del sw, no se puedan realizar las actividades diarias (p.e. envío y recepción de solicitudes por por parte del cliente) generando improductividad en el negocio.	5	4	8
			Software nuevo o inmaduro									
			Falta o insuficiencia de la prueba del software	Abuso de los derechos	IDR266	Insuficientes pruebas	Accesos no autorizados	Pérdida de la integridad de la información / Robo de información	Acceso no autorizado pudiendo generar indisponibilidad del acceso a los aplicativos, pérdida de la integridad de la infrmación	5	4	8
			Defectos bien conocidos en el software									
			Configuración incorrecta de parámetros	Error en el uso	IDR267	Falta de documentación	Procesamiento de data ilegal	Pérdidas financieras	Pérdida en la itnegridad de la información	5	4	8
			Falta de documentación									
			Habilitación de servicios innecesarios	Procesamiento ilegal de datos								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A13	Personal de soporte	Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal	IDR268	Personal desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a que el personal desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	5	4	8
			Falta de conciencia acerca de la seguridad	Error en el uso								
			Falta de políticas para el uso de correo electrónico	Uso no autorizado del equipo	IDR269	Falta de políticas sobre el uso de correo electrónico	Ataques informáticos	Incumplimiento de la ley	Por falta de políticas para el uso del correo electrónico, se generen debilidades y vulnerabilidades de seguridad (ataques informáticos) y se divulgue información o se pierda la integridad de la misma	5	4	8
		Organización	Falta de disposiciones (con respecto a la seguridad) en los contratos con terceros	Abuso de los derechos	IDR270	Información de la Central sin OWNER	Información sin evaluación de seguridad	Falta de detección de vulnerabilidades	Debido a que no se tenga asignado un "OWNER" para la información de la Central que se encuentra registrada en los aplicativos, dicha información no tenga una evaluación de seguridad en términos de confidencialidad, integridad, disponibilidad y privacidad de la información, pudiendo dejarse de detectar vulnerabilidades.	5	4	8
			Falta de procedimiento de monitoreo de los recursos de procesamiento información	Abuso de los derechos								
			Falta de reportes sobre fallas incluidos en los registros de administradores y operador	Abuso de los derechos								
			Falta de procedimientos para la introducción del software en los sistemas operativos	Error en el uso								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A83	Laptop	Hardware	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento	IDR271	Falta de mantenimiento	Mal funcionamiento del equipo	Impacto en la productividad	Debido a faltas de procedimientos y políticas de almacenamiento, genere un mal funciomamiento en el equipo e indisponibilidad de este para ejecutar las actividades cotidianas, impactandose la productividad de la empresa	5	4	8
			Almacenamiento sin protección	Hurto de equipo	IDR272	Inadecuados procedimientos de custodia	Acceso a personal no autorizado a equipos criticos	Indisponibilidad y/o falta de integridad de información / Robo	Debido a inadecuados procedimientos de custodia, personal no autorizado tenga acceso a equipos , pudiendo afectar la disponibilidad e integridad de la información o robo del equipo	5	4	8
			Falta de control de los activos que se encuentran fuera de las instalaciones									
		Organización	Falta de política formal sobre la utilización de computadores portátiles									
A84	Zonas de acceso reservado	Personal	Entrenamiento insuficiente en seguridad al personal	Ingreso de personal no autorizado	IDR273	Inadecuada gestión de accesos	Personal no autorizado acceda zonas restringidas	Daño a equipos y/o robo de información	Debido a una inadecuada gestión de los accesos en la edificación, personal no autorizado pueda acceder, pudiendo provocar daños a equipos y/o robo de información.	5	3	7
			Trabajo no supervisado del personal externo o de limpieza	Hurto de activos								
		Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de activos								
			Falta de protección física de las puertas y ventanas de la edificación	Hurto de activos								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A72	Documento excel Calendario	Software	Falta de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos	IDR274	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Pérdidas finacieras	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a información confidencial	4	3	6
			Trabajo no supervisado del personal externo o de limpieza	Hurto de infomación	IDR275	Actitud del personal	Acceso no autorizado	Fuga y/o robo de información generando pérdidas financieras	Personal de actitud deshonesta acceda al documento, o personal no autorizado logre acceder por un mal funcionamiento, generándose pérdida de la intgegridad o robo de información	4	3	6
			Falta de mecanismos de identificación y autentificación									
A85	Reportes Excel del Servicio Complementario brindado	Software	Falta de protección física de las puertas	Hurto de documentos	IDR276	Actitud del personal	Acceso no autorizado	Fuga y/o robo de información generando pérdidas financieras	Personal de actitud deshonesta acceda al documento, o personal no autorizado logre acceder por falta de políticas de seguridad y monitoreo, generándose pérdida de la intgegridad o robo de información	4	3	6
			Entrenamiento insuficiente en seguridad	Error en el uso								
			Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos								
			Falta de autorización de los recursos de procesamiento de la información	Hurto de documentos								
			Falta de mecanismos de permisos para el acceso al documento									

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A07	Aplicación Ventas	Software	Gestión deficiente de las contraseñas	Falsificación de derechos	IDR277	Inadecuadas políticas de almacenamiento de passwords	Contraseñas accesadas por personal no autorizado	Pérdidas financieras y fuga de información	Debido a inadecuadas políticas de almacenamiento de passwords, las contraseñas al Módulo de Ventas sean accesadas por personal no autorizado, pudiendo provocar fuga de información y grandes pérdidas financieras	5	2	6
			Falta de control eficaz del cambio	Mal funcionamiento del software	IDR278	Errores en el sw	Inadecuada segregación de funciones	Controles sin efectividad	Debido a errores en el sw se produzca una mala asignación de perfiles definidos para los roles del personal y no exista una adecuada segregación de funciones para los procesos de negocio, por lo que los controles de los procesos pierdan efectividad.	5	2	6
			Falta de copias de respaldo	Manipulación del software	IDR279	Mal funcionamiento	Operativa impactada de los procesos de negocio	Impacto en productividad del negocio	Por falta de respaldo o un control eficaz del software, se afecte la operativa de los procesos de negocio soportados y por ende la productividad del negocio.	5	3	7
		Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos								
A76	Documento Word de la cotización	Software	Falta de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos	IDR280	Falta de políticas de otorgamiento de accesos	Acceso no autorizado	Pérdida de integridad / Robo	Debido a una inadecuada gestión de accesos, se otorguen mayores accesos a los usuarios de los que se definieron inicialmente o accesos a usuarios no autorizados , posibilitando la pérdida de integridad de la información o robo de información debido al interés de la competencia.	5	3	7
			Trabajo no supervisado del personal externo o de limpieza	Hurto de infomación								
			Falta de mecanismos de permisos para el acceso al documento									

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A65	Contrato (Clientes)	Organización	Falta de revisiones en las disposiciones por parte de la gerencia	Usos no autorizados de hardware y software	IDR281	Falta de revisión de contratos a personal y clientes	Fraude	Pérdida financiera	Debido a una falta de revisión de las disposiciones en los contratos, no se establezcan medidas de seguridad para con los clientes, generando fraudes ,y/o hurto de información o equipos sin la posibilidad de recibir una indemnización por la pérdida financiera generada	5	3	7
				Hurto de equipos, documentos o/y información								
				Abuso de los derechos								
A70	Datamart	Software	Falta de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos	IDR282	Inadecuados procesos de detección	Intentos no autorizados de acceso a información	Error en los mecanismos de detección de ataques internos/externos / Pérdidas financieras	Debido a inadecuados procesos de detección, los intentos no autorizados de acceso a información del Datamart no sean detectados y se produzcan ataques informáticos	5	3	7
			Falta de copias de respaldo	Manipulación con software								
A71	Host	Hardware	Falta de planes de continuidad	Falla del equipo	IDR283	Inadecuados procedimientos de custodia	Acceso a personal no autorizado a equipos criticos	Indisponibilidad y/o falta de integridad de información	Debido a inadecuados procedimientos de custodia, personal no autorizado tenga acceso al Host, el cual procesa toda la información crítica del negocio, impactando gravemente en la disponibilidad, confidencialidad e integridad de la información.	5	2	6
			Falta de procedimiento de monitoreo	Abuso de los derechos								
			Falta de procedimientos de identificación y evaluación de riesgos									
			Falta de reportes sobre fallas		IDR284	Inadecuada gestión de accesos	Personal no autorizado acceda al CC	Daño a equipos y/o robo de información	Debido a una inadecuada gestión de los accesos en el centro de cómputo, personal no autorizado pueda acceder, pudiendo provocar daños a equipos y/o robo de información.	5	2	6

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A54	Aplicación para la depuración y enriquecimiento de Data	Software	Falta de control eficaz del cambio	Mal funcionamiento del software	IDR287	Errores en el sw	Inadecuada segregación de funciones	Controles sin efectividad	Debido a errores en el sw se produzca una mala asignación de perfiles definidos para los roles del personal y no exista una adecuada segregación de funciones para los procesos de negocio, por lo que los controles de los procesos pierdan efectividad.	4	2	5
			Especificaciones incompletas o no claras para los desarrolladores									
			Gestión deficiente de las contraseñas	Falsificación de derechos	IDR288	Falta de identificación de usuarios / logs insuficientes	Imposibilidad de identificar a usuario	No sea posible tomar acción correctiva	Debido a la falta de mecanismos de autenticación e identificación de usuarios / logs insuficientes, no sea posible identificar a usuario y por ende no sea posible tomar acción correctiva.	4	3	6
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario									
			Configuración incorrecta de parámetros	Error en el uso	IIDR289	Fallas en la gestión de la documentación	Información no disponible	Pérdida de Integridad en la información, fuga de información, divulgación	Por falta de documentación (manuales, procedimientos, reporte de turnos e indicadores de gestión), haya la posibilidad de fallas en el otorgamiento de accesos generando fuga de información	3	2	4
			Falta de documentación									
			Distribución errada de los derechos de acceso	Abuso de los derechos	IDR290	Inadecuada gestión de accesos	Usuarios con mas accesos de los definidos inicialmente	Impacto en productividad del negocio	Debido a la falta de pruebas en el software traiga como consecuencia una inadecuada gestión de accesos y se otorguen mayores accesos a los usuarios de los que se definieron inicialmente, posibilitando el uso incorrecto de los mismos.	4	2	5
			Falta de "terminación de la sesión" cuando se abandona la estación de trabajo									
			Defectos bien conocidos en el software									
			Falta o insuficiencia de la prueba del software									

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A55	Cámaras de vigilancia	Hardware	Susceptibilidad al polvo, suciedad	Mal funcionamiento del equipo	IDR291	Falta de mantenimiento	Fallas en el funcionamiento	Pérdidas financieras	Debido a insuficientes políticas de mantenimiento falle el funcionamiento de las cámaras y no se pueda efectuar acciones correctivas o controles necesarios dentro del área de operaciones	3	2	4
				Destrucción del equipo, corrosión								
			Susceptibilidad a la temperatura	Mal funcionamiento del equipo								
				Destrucción del equipo, corrosión								
A30	Intranet de la Central de Riesgo	Software	Interfaz de usuario complicada	Error en el uso	IDR285	Incumplimiento del procedimiento	Desbloqueo de un usuario de forma constante	Bloqueo reiteraivo y/o ataque mayor	Debido al incumplimiento del procedimiento, se desbloquee un usuario de forma constante sin validar que este sea victima de un ataque externo o interno, se genere un bloqueo reiterativo de usuario y/o ataque mayor.	5	3	7
			Falta de documentación y actualización de dicha documentación									
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos	IDR286	Errores en el procedimiento de baja de usuarios	Accesos a usuarios no autorizados	Robo y/o fuga de información	Debido a errores en el procedimiento de baja de usuarios, no se dé de baja o bloquee los accesos a un usuario que cambia de puesto de trabajo, posibilitando el robo y/o fuga de información.	5	3	7
			Gestión deficiente de las contraseñas									
		Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos								

4. Matriz de Riesgos: Generar Servicios Etapa Prospección

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A19	Correo electrónico	Personal	Falta de políticas para el uso del correo electrónico	Uso no autorizado del equipo	IDR80	Personal de la Central de Riesgo desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a que el personal de la Central de Riesgo desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internas relacionadas con el uso de correo electrónico pudiendo generar debilidades y vulnerabilidades de seguridad.	5	3	7
			Entrenamiento insuficiente en seguridad	Error en el uso								
		Organización	Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Abuso de los derechos	IDR81	Inadecuado procedimiento de contratación y disposiciones en contrato	Incorrecto uso de correo electrónico	Vulnerabilidad de seguridad	Debido a un inadecuado procedimiento de contratación como la evidencia de antecedentes penales y policiales, desarrollo de pruebas de competencia, desconocimiento de las normas, políticas y criterios de seguridad de información y falta de disposiciones en contratos se incumplan las normas internas pudiendo generar debilidades y vulnerabilidades en la seguridad de la Central de Riesgo.	5	4	8
			Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Falsificación y Abuso de derechos	IDR82	Falta de procesos disciplinarios	Ataques informáticos	Pérdida en la integridad de la Información, Robo / divulgación de la información	Debido a la falta de procesos disciplinarios en caso de incidentes de seguridad a través del uso del correo electrónico no sea posible tomar acciones correctivas.	5	3	7
A20	Servidor de Correo	Hardware	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información	IDR83	Falta de mantenimiento	Acceso a la BD interrumpido	Operativa impactada de los procesos de negocio, improductividad/ Pérdidas financieras	Debido a la falta de mantenimiento, el acceso a la Base de Datos se vea interrumpido	5	5	9
			Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento								
			Almacenamiento sin protección	Hurto de información	IDR84	Inadecuado procedimiento de custodia de equipos y como consecuencia de información confidencial	Información confidencial accesada por personal no autorizado	Acceso y/o divulgación de información confidencial	Debido a inadecuados procedimientos de custodia y falta de procedimientos para copias, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio, pudiendo afectar la disponibilidad e integridad de la información.	5	4	8
			Copia no controlada	Hurto de información								
		Lugar	Falta de protección física de las puertas y ventanas de la edificación	Hurto de Servidor								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A29	Servidores de Archivos	Hardware	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información	IDR85	Falta de mantenimiento	Acceso a la BD interrumpido	Operativa impactada de los procesos de negocio, improductivadad/ Pérdidas financieras	Debido a la falta de mantenimiento, el acceso a la Base de Datos se vea interrumpido	5	2	6
			Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento								
			Almacenamiento sin protección	Hurto de información	IDR86	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso personal no autorizado tenga acceso a los servidores de archivos que contienen nformación crítica para el negocio, pudiendo afectar la integridad y/o disponibilidad de la información.	4	3	6
			Copia no controlada									
		Lugar	Falta de protección física de las puertas y ventanas de la edificación	Hurto de Servidor	IDR87	Inadecuados procedimientos de custodia	Acceso a personal no autorizado a equipos criticos	Indisponibilidad y/o falta de integridad de información	Debido a inadecuados procedimientos de custodia, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio de la Central, pudiendo afectar la disponibilidad e integridad de la información.	5	3	7
		Organización	Falta de autorización de los recursos de procesamiento de la información									
			Falta de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo	IDR88	Falta de políticas de custodia de equipos	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a la falta de políticas internas, personal no autorizado acceda a iinformación crítica.	4	3	6

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A43	Aplicación para generar Modelos Estadísticos	Software	Distribución errada de los derechos de acceso	Abuso de los derechos	IDR89	Falta de políticas de otorgamiento de accesos	Indisponibilidad de servicio	Pérdidas financieras	Acceso no autorizado pudiendo generar indisponibilidad del acceso al aplicativo	4	3	6
			Falta de procedimiento formal para el registro y retiro del registro de usuario									
			Falta de documentación y actualización de dicha documentación	Error en el uso	IDR90	Fallas en la gestión de la documentación	Información no disponible	Pérdida de Integridad en la información, fuga de información, divulgación	Por falta de documentación (manuales, procedimientos, reporte de turnos e indicadores de gestión), haya la posibilidad de fallas en el otorgamiento de accesos generando fuga de información	4	2	5
			Configuración incorrecta de parámetros									
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos	IDR91	Falta de procedimientos y políticas de seguridad	Ataques informaticos a aplicaciones del negocio	ndisponibilidad y/o falta de integridad de las aplicaciones	Debido a la falta de autentificación personal no autorizado acceda al aplicativo y se produzcan ataques a la aplicación	4	3	6
			Gestión deficiente de las contraseñas									
		Personal	Uso incorrecto de software	Error en el uso								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A44	Aplicación Georeferenciada	Software	Distribución errada de los derechos de acceso	Abuso de los derechos	IDR92	Inadecuada gestión de accesos	Usuarios con mas accesos de los definidos inicialmente	Impacto en productividad del negocio	Debido a la falta de pruebas en el software traiga como consecuencia una inadecuada gestión de accesos y se otorguen mayores accesos a los usuarios de los que se definieron inicialmente, posibilitando el uso incorrecto de los mismos.	4	3	6
			Falta de documentación y actualización de dicha documentación	Error en el uso								
			Configuración incorrecta de parámetros									
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos								
			Gestión deficiente de las contraseñas									
		Personal	Uso incorrecto de software	Error en el uso	IDR93	Falta de identificación de usuarios / logs insuficientes	Imposibilidad de identificar a usuario	No sea posible tomar acción correctiva	Debido a la falta de mecanismos de registro de usuarios haya logs insuficientes y no sea posible identificar a usuario y por ende no sea posible tomar acción correctiva.	4	2	5
		Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A17	Portal Web	Software	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos	IDR94	Fallas en el Sistema	Ingreso no Autorizado	Pérdida en la integridad de la Información	Personas no autorizadas ingresen al Portal, manipulándolo y causando pérdidas en la integridad de la información	5	2	6
			Distribución errada de los derechos de acceso									
			Interfase de usuario complicada	Error en el uso	IDR95	Errores en la asignación de perfiles	Inadecuada segregación de funciones	Controles sin efectividad	Debido a errores en la asignación de perfiles definidos para los roles del personal por tener una interfaz complicada para el Portal Web, no exista una adecuada segregación de funciones para los procesos de negocio, por lo que los controles de los procesos pierdan efectividad.	5	2	6
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos	IDR96	Inadecuadas políticas de almacenamiento de passwords	Contraseñas maestras accesadas por personal no autorizado	Inadecuados niveles de servicio y/o fuga de información	Debido a inadecuadas políticas de almacenamiento de passwords, las contraseñassean accesadas por personal no autorizado, pudiendo afectar los niveles de servicio y/o provocar fuga de información.	5	2	6
			Gestión deficiente de las contraseñas									
			Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR97	Actitud deshonesta del personal y/o falta de procedimiento de baja de usuarios	Accesos a usuarios no autorizados	Robo y/o fuga de información	Debido a actitud deshonesta del personal, exista fraude interno al no realizar las bajas o cambios de roles oportunamente, generandose fuga y/o robo de información. O por no seguir un procedimiento formal se bloqueen los accesos a un usuario que cambia de puesto de trabajo.	5	2	6

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A16	Base de Datos Microsoft Sql Server 2003 - 2008	Software	Falta o insuficiencia de la prueba del software Defectos bien conocidos en el software Falta de pruebas de auditoría Distribución errada de los derechos de acceso	Abuso de los derechos	IDR98	Falta de logs	Intentos de acceso no autorizados	Ataques informáticos, pérdida financiera	Debido a insuficientes logs de auditoría, los intentos no autorizados de acceso a la Base de Datos no sean detectados y se produzcan ataques informáticos.	5	3	7
A28	Servidores de Base de Datos	Hardware	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información	IDR99	Falta de mantenimiento	Acceso a la BD interrumpido	Operativa impactada de los procesos de negocio, improductividad/ Pérdidas financieras	Debido a la falta de mantenimiento, el acceso a la Base de Datos se vea interrumpido	5	2	6
			Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento								
			Almacenamiento sin protección	Hurto de información	IDR100	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso (por ejem: fallas en custodia de archivos que contiene los passwords de los usuarios genéricos de aplicación del ambiente de producción,) personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio, pudiendo afectar la integridad y/o disponibilidad de la información.	5	2	6
			Uso inadecuado o descuidado del control de acceso físico a las edificaciones	Destrucción de equipo o medios								
			Copia no controlada	Hurto de información								
		Lugar	Falta de protección física de las puertas y ventanas de la edificación	Hurto de Servidor	IDR101	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio de la Central como los Servidores, pudiendo afectar la integridad y/o disponibilidad de la información.	5	2	6

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A85	Documentos - Reportes Excel	Software	Falta de protección física de las puertas	Hurto de documentos	IDR102	Actitud del personal	Acceso no autorizado	Fuga y/o robo de información generando pérdidas financieras	Personal de actitud deshonesta acceda al documento, o personal no autorizado logre acceder por falta de políticas de seguridad y monitoreo, generándose pérdida de la intgegridad o robo de información	4	3	6
			Entrenamiento insuficiente en seguridad	Error en el uso								
			Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos								
			Falta de autorización de los recursos de procesamiento de la información	Hurto de documentos								
			Falta de mecanismos de permisos para el acceso al documento									
A46	Piezas de Marketing como servicio al Cliente *(Brochures)*	Personal	Trabajo no supervisado del personal externo o de limpieza	Hurto de documentos	IDR103	Inadecuadas políticas de acceso	Acceso no autorizado	Pérdidas financieras	Debido a inadecuadas políticas de accesos, personal no autorizado acceda a la información confidencial de la empresa (Publicidad) y altere o modifique la data, ocasionando pérdida de la integridad de la información	4	2	5
			Entrenamiento insuficiente en seguridad	Error en el uso								
		Organización	Falta de procedimientos para el manejo de información clasificada									
			Falta o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de documentos								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A24	CD encriptado	Hardware	Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del CD Polvo, corrosión	IDR104	Inadecuadas políticas de almacenamiento	Información no disponible	Impacto en productividad del negocio, incumplimiento de contrato, incumplimiento de la ley	Por inadecuadas políticas de almacenamiento, se dañen CDs que almacenan información crítica para el negocio de la Central, pudiendo afectar la integridad y/o disponibilidad de la información.	5	3	7
			Almacenamiento sin protección	Hurto o destrucción de CD	IDR105	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a los Cds que almacenan información crítica para el negocio de la Central de Riesgo, pudiendo afectar la integridad y/o disponibilidad de la información o Robo	5	2	6
			Copia no controlada									
		Personal	Trabajo no supervisado del personal externo o de limpieza									
A48	Web Service	Software	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software	IDR106	Falla en el funcionamiento	Falla en los servicios	Pérdidas financieras / Incumplimiento de contrato	Debido al mal funcionamiento del sw, no se puedan realizar las actividades diarias (p.e. envío y recepción de solicitudes por por parte del cliente) generando improductividad en el negocio.	5	3	7
			Software nuevo o inmaduro									
			Falta o insuficiencia de la prueba del software	Abuso de los derechos	IDR107	Insuficientes pruebas	Accesos no autorizados	Pérdida de la integridad de la información / Robo de información	Acceso no autorizado pudiendo generar indisponibilidad del acceso a los aplicativos, pérdida de la integridad de la infrmación	5	3	7
			Defectos bien conocidos en el software									
			Configuración incorrecta de parámetros	Error en el uso	IDR108	Falta de documentación	Procesamiento de data ilegal	Pérdidas financieras	Pérdida en la itnegridad de la información	5	2	6
			Falta de documentación									
			Habilitación de servicios innecesarios	Procesamiento ilegal de datos								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A52	Personal de Tecnología como Servicio	Personal	Entrenamiento insuficiente en seguridad	Hurto de información	IDR109	Personal desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad / Robo de información / Divulgación / Pérdida de Integridad	Debido a que el personal de la Central desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	5	4	8
			Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo								
		Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR110	Fallas en la revisión de las bajas de los perfiles	Personas no autorizadas con accesos	Fuga y/o robo de información	Debido a fallas en el proceso de bajas de los perfiles de usuarios , personas a las que no corresponde cuenten con accesos a los que ya no están autorizados, pudiendo generarse fuga y/o robo de información.	5	3	7
			Falta de proceso formal para la revisión (supervisión) de los derechos de acceso									
			Falta de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones	IDR111	Falta de designación de owners	Se otorguen o eliminen accesos sin aprobaciones	Divulgación de información / pérdidas financieras	Debido a que no se cuenta con una relación de aplicativos (cliente/servidor y host) vs. owners, se otorguen o eliminen accesos sin contar con todas las aprobaciones requeridas, pudiendo facilitar la divulgación de información y el hurto de Información, ocasionando grandes pérdidas financieras	5	3	7
			Falta de políticas sobre el uso del correo electrónico	Error en el uso								
			Falta de procedimientos para la introducción del software en los sistemas operativos									
			Falta de procedimientos para el manejo de información clasificada									
			Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos								
			Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo o información								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A65	Contrato (Clientes)	Organización	Falta de revisiones en las disposiciones por parte de la gerencia	Usos no autorizados de hardware y software	IDR112	Falta de revisión de contratos a personal y clientes	Fraude	Pérdida financiera	Debido a una falta de revisión de las disposiciones en los contratos, no se establezcan medidas de seguridad para con los empleados, generando fraudes ,y/o hurto de información o equipos sin la posibilidad de recibir una indemnización por la pérdida financiera generada	5	2	6
				Hurto de equipos, documentos o/y información								
				Abuso de los derechos								
A78	Personal Servicio al Cliente	Personal	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo	IDR113	Actitud deshonesta del personal	Accesos inadecuados	Fuga y/o robo de información	Debido a actitud deshonesta del personal, exista fraude interno al no realizar las bajas o cambios de roles oportunamente, generandose fuga y/o robo de información.	5	4	8
			Ausencia del personal	Incumplimiento en la disponibilidad del personal								
A46	Manual de uso de Aplicación para generar Modelos Estadísticos	Organización	Falta de políticas para la utilización de activos de la empresa	Error en el uso	IDR114	Fallas en la gestión de la documentación	Información no disponible	Copia no autorizada / Divulgación de la información	Por fallas en la gestión (almacenamiento) de la documentación (manuales, procedimientos, reporte de turnos e indicadores de gestión), esta no se encuentre disponible o pueda ser accedido por personal no autorizado, facilitando su copia a hurto	4	4	7
				Hurto del manual o copias ilegales								
			Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Copiado del software o el manual								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A47	Manual de uso de Aplicación Aplicación Georeferenciada	Organización	Falta de políticas para la utilización de activos de la empresa	Error en el uso	IDR115	Fallas en la gestión de la documentación	Información no disponible	Copia no autorizada / Divulgación de la información	Por fallas en la gestión (almacenamiento) de la documentación (manuales, procedimientos, reporte de turnos e indicadores de gestión), esta no se encuentre disponible o pueda ser accedido por personal no autorizado, facilitando su copia a hurto	4	4	7
				Hurto del manual o copias ilegales								
			Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Copiado del software o el manual								
A53	Aplicación Web de Preselección	Software	Falta o insuficiencia de la prueba del software	Abuso de los derechos	IDR116	Inadecuada gestión de accesos	Usuarios con mas accesos de los definidos inicialmente	Impacto en productividad del negocio	Debido a la falta de pruebas en el software traiga como consecuencia una inadecuada gestión de accesos y se otorguen mayores accesos a los usuarios de los que se definieron inicialmente, posibilitando el uso incorrecto de los mismos.	4	2	5
			Falta de pruebas de auditoría									
			Falta de documentación	Error en el uso								
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos								
			Gestión deficiente de las contraseñas									
			Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software	IDR117	Errores en el sw	Inadecuada segregación de funciones	Controles sin efectividad	Debido a errores en el sw se produzca una mala asignación de perfiles definidos para los roles del personal y no exista una adecuada segregación de funciones para los procesos de negocio, por lo que los controles de los procesos pierdan efectividad.	4	2	5

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A51	Personal de Tecnología de Información	Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal	IDR118	Inadecuados procesos de contrtación y falta de capacitación	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información / Pérdidas finacieras /Robo de información	Debido a que el personal desconozca las normas, políticas y criterios de seguridad de información, y en algunos casos debido a procedimientos inadecuados de contratación, se incumplan las normas internas pudiendo generar debilidades y vulnerabilidades de seguridad, errores en el uso de aplicativos, ypérdida de integridad de la información e incluso hurto y fraude.	5	4	8
			Procedimientos inadecuados de contratación	Destrucción de equipos o medios								
			Entrenamiento insuficiente en seguridad	Error en el uso								
			Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos								
			Trabajo no supervisado	Hurto de información o medios								
		Lugar	Falta de protección física de las puertas	Hurto de equipo	IDR119	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso físico, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio (medios de almacenamiento) pudiendo afectar la integridad y/o disponibilidad de la información.	5	3	7
		Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR120	Falta de segregación de funciones	Unidad sea responsable de definir/crear/aprobar cambios	Errores y/o abuso de funciones	Debido a falta de segregación de funciones, una misma unidad sea responsable de definir, crear y aprobar cambios en producción relacionado a roles, ocasionando errores y/o abuso de funciones.	5	3	7
			Falta de proceso formal para la revisión (supervisión) de los derechos de acceso									
			Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con terceros									
			Falta o insuficiencia en el acuerdo a nivel de servicio	Incumplimiento en el mantenimiento del sistema de información	IDR121	Falta de mantenimiento	Falla en los aplicativos	Acceso no autorizados, robo de información	Fallas en el funcionamiento de los aplicativos generando vulnerabildiades en la seguridad, accesos no autorizados, robo de información.	5	3	7

5. Matriz de Riesgos: Generar Etapa Admisión

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A48	Web Service	Software	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software	IDR166	Falla en el funcionamiento	Falla en los servicios	Pérdidas financieras / Incumplimiento de contrato	Debido al mal funcionamiento del sw, no se puedan realizar las actividades diarias (p.e. envío y recepción de solicitudes por por parte del cliente) generando improductividad en el negocio.	5	3	7
			Software nuevo o inmaduro									
			Falta o insuficiencia de la prueba del software	Abuso de los derechos	IDR167	Insuficientes pruebas	Accesos no autorizados	Pérdida de la integridad de la información / Robo de información	Acceso no autorizado pudiendo generar indisponibilidad del acceso a los aplicativos, pérdida de la integridad de la infrmación	5	2	6
			Defectos bien conocidos en el software									
			Configuración incorrecta de parámetros	Error en el uso	IDR168	Falta de documentación	Procesamiento de data ilegal	Pérdidas financieras	Pérdida en la itnegridad de la información	5	2	6
			Falta de documentación									
			Habilitación de servicios innecesarios	Procesamiento ilegal de datos								
A62	Servidor FTP	Hardware	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario cifrados	Falsificación de derechos	IDR169	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso personal no autorizado tenga acceso a pudiendo afectar la integridad y/o disponibilidad de la información.	4	4	7
				Corrupción de datos								
				Hurto de información								
A64	Verificadores	Personal	Uso incorrecto de los equipos móviles	Error en el uso	IDR170	Inadecuadas políticas de acceso y monitoreo	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso personal externo tenga acceso a equipos o documentación que almacenan o procesan información crítica para el negocio del Banco, pudiendo afectar la integridad y/o disponibilidad de la información.	5	3	7
				Procesamiento ilegal de datos								
			Falta de capacitación para la realización de sus actividades	Error en el uso de equipo								
			Trabajo no supervisado	Hurto de equipos								
			Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos								
			Falta de proceso formal para la revisión (supervisión) de los derechos de acceso									
			Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los verificadores	Procesamiento ilegal de datos	IDR171	Personal desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Por falta de capacitación a verificadores se procese información incorrecta o se incumplan normas internas pudiendo generar vulnerabilidades en la seguridad como robo de equipo.	4	5	8
			Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo o información								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A77	Aplicación de Verificaciones	Software	Falta o insuficiencia de la prueba del software	Abuso de los derechos	IDR172	Inadecuados procesos de detección	Intentos no autorizados de acceso a información	Debido al Robo o fuga de información haya pérdidas financieras	Debido a un mal funcionamiento del aplicativo web podrían haber intentos no autorizados de acceso que no sean detectados y se produzcan ataques informáticos, lo que conlleva a robo o fuga de información	5	3	7
			Defectos bien conocidos en el software	Error en el uso	IDR173	Fallas en el aplicativo Web	Falla en los accesos	Imposibilidad de ejecutar labores	Debido a fallas en aplicativo web (por ejm: el personal podría no contar con accesos disponibles) se imposibiliten las labores cotidianas trayendo pérdidas financieras para la empresa e improductividad	4	2	5
			Distribución errada de los derechos de acceso									
			Falta de documentación									
			Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software	IDR174	Fallas en el aplicativo Web	Usuarios no autorizados ingresen al sistema	Falta de integridad y/o disponibilidad de la información	Debido a fallas de terminación de sesión del aplicativo Web, usuarios a quienes no le corresponden acceso, ingresen al sistema pudiendo afectar la integridad y/o disponibilidad de la información.	5	1	5
			Falta de control eficaz del cambio									
			Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR175	Falta de identificación de usuarios / logs insuficientes	Imposibilidad de identificar a usuario	No sea posible tomar acción correctiva	Debido a la falta de mecanismos de autenticación e identificación de usuarios / logs insuficientes, no sea posible identificar a usuario y por ende no sea posible tomar acción correctiva.	5	2	6
		Organización	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Copia de software - mal funcioamiento	IDR176	Falta de procedimientos	Robo	Pérdidas financieras	Debido a la falta de protección física en las puertas se produzca robo de información, fuga o divulgación lo que conlleve a pérdidas financieras	5	1	5

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A81	Personal Operaciones	Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal	IDR177	Incumplimiento de procedimientos	Ataques informaticos a aplicaciones del negocio	Indisponibilidad y/o falta de integridad de las aplicaciones	Por procedimientos inadecuados de contratación y falta de mecanismos de monitorei, se produzcan ataques informáticos a aplicaciones del negocio, o a equipos como servidores pudiendo provocar indisponibilidad y/o falta de integridad de las aplicaciones e información de Titulares	5	3	7
			Procedimientos inadecuados de contratación	Destrucción de equipos o medios								
			Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos								
A63	Sistema de decisiones	Software	Software de distribución amplia	Corrupción de datos	IDR178	Interfaz complicada / Falta de documentacion	Errores en el uso de aplicativos	Acceso no autorizados, robo de información	Debido a la falta de documentacion , halla una una falla en la designación de perfiles y roles y configuración de parámetros pudiendo generar fallas en la entrega del servicio, improductividad y accesos no autorizados.	5	2	6
			Interfase de usuario complicada	Error en el uso	IDR179	Falla en el funcionamiento	Acceso no autorizado	Ataques informáticos / Pérdidas financieras	Fallas en el funcionamiento de los aplicativos generando vulnerabildiades en la seguridad, accesos no autorizados, robo de información.	5	3	7
			Falta de documentación									
			Configuración incorrecta de parámetros									
			Falta de control eficaz del cambio	Mal funcionamiento del software								
A24	CD encriptado	Hardware	Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del CD Polvo, corrosión	IDR180	Inadecuadas políticas de almacenamiento	Información no disponible	Impacto en productividad del negocio, incumplimiento de contrato, incumplimiento de la ley	Por inadecuadas políticas de almacenamiento, se dañen CDs que almacenan información crítica para el negocio de la Central, pudiendo afectar la integridad y/o disponibilidad de la información.	4	3	6
			Almacenamiento sin protección	Hurto o destrucción de CD	IDR181	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a los Cds que almacenan información crítica para el negocio de la Central de Riesgo, pudiendo afectar la integridad y/o disponibilidad de la información o Robo	4	3	6
			Copia no controlada									
		Personal	Trabajo no supervisado del personal externo o de limpieza									

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A17	Portal Web	Software	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo Distribución errada de los derechos de acceso	Abuso de los derechos	IDR182	Fallas en el Sistema	Ingreso no Autorizado	Pérdida en la integridad de la Información	Personas no autorizadas ingresen al Porta, manipulándolo y causando pérdidas en la integridad de la información	5	3	7
			Interfase de usuario complicada / Falta de control de cambios	Falta de mantemiento / Error en el uso	IDR183	Errores en la asignación de perfiles	Inadecuada segregación de funciones	Controles sin efectividad	Debido a errores en la asignación de perfiles definidos para los roles del personal por tener una interfaz complicada para el Portal Web, no exista una adecuada segregación de funciones para los procesos de negocio, por lo que los controles de los procesos pierdan efectividad.	5	3	7
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario Gestión deficiente de las contraseñas	Falsificación de derechos	IDR184	Inadecuadas políticas de almacenamiento de passwords	Contraseñas maestras accesadas por personal no autorizado	Inadecuados niveles de servicio y/o fuga de información	Debido a inadecuadas políticas de almacenamiento de passwords, las contraseñassean accesadas por personal no autorizado, pudiendo afectar los niveles de servicio y/o provocar fuga de información.	5	3	7
			Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR185	Actitud deshonesta del personal y/o falta de procedimiento de baja de usuarios	Accesos a usuarios no autorizados	Robo y/o fuga de información	Debido a actitud deshonesta del personal, exista fraude interno al no realizar las bajas o cambios de roles oportunamente, generandose fuga y/o robo de información. O por no seguir un procedimiento formal se bloqueen los accesos a un usuario que cambia de puesto de trabajo.	5	3	7
A16	Base de Datos Microsoft Sql Server 2003 - 2008	Software	Falta o insuficiencia de la prueba del software Defectos bien conocidos en el software Falta de pruebas de auditoría	Abuso de los derechos	IDR186	Falta de logs	Intentos de acceso no autorizados	Ataques informáticos	Debido a insuficientes logs de auditoría, los intentos no autorizados de acceso a la Base de Datos no sean detectados y se produzcan ataques informáticos.	5	2	6
			Distribución errada de los derechos de acceso		IDR187	Inadecuado procedimiento de identificación de funciones	Definición incorrecta de perfiles de acceso	Usuarios tengan accesos de más o restringidos	Debido a un inadecuado procedimiento de identificación de funciones, no se realice correctamente la definición de los perfiles de accesos y por ende los usuarios tengan accesos de más o restringidos.	4	2	5

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A61	Aplicación B2B	Software	Defectos bien conocidos en el software	Abuso de los derechos	IDR188	Falta de pruebas	Falla en el servicio	Pérdidas financieras	Debido a fallas en la aplicación no se llegue a brindar el servicio	4	3	6
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos								
			Tablas de contraseñas sin protección									
A60	Equipo móvil Nextel	Hardware	Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo. Polvo, corrosión, congelamiento	IDR189	Falta de capacitaciones	Falla en el servicio	Información no disponible / incumplimiento de contrato	Debido a falta de capacitaciones a empleados en seguridad y empleo de activos, se dañen o roben.	4	4	7
			Falta de cuidado en la disposición final	Hurto de equipo								
		Personal	Uso incorrecto de software y hardware	Error en el uso								
			Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo								
A51	Personal de la Tecnología de la Información	Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal	IDR190	Inadecuados procesos de contrtación y falta de capacitación	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información / Pérdidas finacieras /Robo de información	Debido a que el personal desconozca las normas, políticas y criterios de seguridad de información, y en algunos casos debido a procedimientos inadecuados de contratación, se incumplan las normas internas pudiendo generar debilidades y vulnerabilidades de seguridad, errores en el uso de aplicativos, ypérdida de integridad de la información e incluso hurto y fraude.	5	4	8
			Procedimientos inadecuados de contratación	Destrucción de equipos o medios								
			Entrenamiento insuficiente en seguridad	Error en el uso								
			Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos								
			Trabajo no supervisado	Hurto de información o medios								
		Lugar	Falta de protección física de las puertas	Hurto de equipo	IDR191	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso físico, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio (medios de almacenamiento) pudiendo afectar la integridad y/o disponibilidad de la información.	5	4	8

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A51	Personal de la Tecnología de la Información	Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR192	Falta de segregación de funciones	Unidad sea responsable de definir/crear/aprobar cambios	Errores y/o abuso de funciones	Debido a falta de segregación de funciones, una misma unidad sea responsable de definir, crear y aprobar cambios en producción relacionado a roles, ocasionando errores y/o abuso de funciones.	5	4	8
			Falta de proceso formal para la revisión (supervisión) de los derechos de acceso									
			Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con terceros									
			Falta o insuficiencia en el acuerdo a nivel de servicio	Incumplimiento en el mantenimiento del sistema de información	IDR193	Falta de mantenimiento	Falla en los aplicativos	Acceso no autorizados, robo de información	Fallas en el funcionamiento de los aplicativos generando vulnerabildiades en la seguridad, accesos no autorizados, robo de información.	5	3	7
A59	Cargo	Organización	Entrenamiento insuficiente en seguridad	Error en el uso	IDR194	Personal desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a que el personal (en especial los couriers) desconozcan las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	4	3	6
			Trabajo no supervisado del personal externo o de limpieza	Hurto de los paquetes								
			Falta de procedimientos para el manejo de información clasificada	Error en el uso								
			Falta de control de los activos que se encuentran fuera de las instalaciones	Hurto de los paquetes								
A52	Personal de Tecnología como Servicio	Personal	Entrenamiento insuficiente en seguridad	Hurto de información	IDR195	Personal desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad / Robo de información / Divulgación / Pérdida de Integridad	Debido a que el personal de la Central desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	4	3	6
			Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A52	Personal de Tecnología como Servicio	Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR196	Inadecuado procedimiento de identificación de funciones	Definición incorrecta de perfiles de acceso	Usuarios tengan accesos de más o restringidos	Debido a un inadecuado procedimiento de identificación de funciones, no se realice correctamente la definición de los perfiles de accesos y por ende los usuarios tengan accesos de más o restringidos.	5	3	7
			Falta de proceso formal para la revisión (supervisión) de los derechos de acceso									
			Falta de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones								
			Falta de políticas sobre el uso del correo electrónico	Error en el uso	IDR197	Falta de designación de owners	Se otorguen o eliminen accesos sin aprobaciones	Divulgación de información / pérdidas financieras	Debido a que no se cuenta con una relación de aplicativos (cliente/servidor y host) vs. owners, se otorguen o eliminen accesos sin contar con todas las aprobaciones requeridas, pudiendo facilitar la divulgación de información y el hurto de Información, ocasionando grandes pérdidas financieras	5	4	8
			Falta de procedimientos para la introducción del software en los sistemas operativos									
			Falta de procedimientos para el manejo de información clasificada									
			Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos								
			Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo o información								

6. Matriz de Riesgos: Generar Etapa Recuperación

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A19	Correo electrónico	Personal	Falta de políticas para el uso del correo electrónico	Uso no autorizado del equipo	IDR122	Personal de la Central de Riesgo desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a que el personal de la Central de Riesgo desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internas relacionadas con el uso de correo electrónico pudiendo generar debilidades y vulnerabilidades de seguridad.	5	3	7
			Entrenamiento insuficiente en seguridad	Error en el uso								
		Organización	Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Abuso de los derechos	IDR123	Inadecuado procedimiento de contratación y disposiciones en contrato	Incorrecto uso de correo electrónico	Vulnerabilidad de seguridad	Debido a un inadecuado procedimiento de contratación como la evidencia de antecedentes penales y policiales, desarrollo de pruebas de competencia, desconocimiento de las normas, políticas y criterios de seguridad de información y falta de disposiciones en contratos se incumplan las normas internas pudiendo generar debilidades y vulnerabilidades en la seguridad de la Central de Riesgo.	5	4	8
			Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Falsificación y Abuso de derechos	IDR124	Falta de procesos disciplinarios	Ataques informáticos	Pérdida en la integridad de la Información, Robo / divulgación de la información	Debido a la falta de procesos disciplinarios en caso de incidentes de seguridad a través del uso del correo electrónico no sea posible tomar acciones correctivas.	5	3	7
A85	Documentos - Reportes Excel	Software	Falta de protección física de las puertas	Hurto de documentos	IDR125	Actitud del personal	Acceso no autorizado	Fuga y/o robo de información generando pérdidas financieras	Personal de actitud deshonesta acceda al documento, o personal no autorizado logre acceder por falta de políticas de seguridad y monitoreo, generándose pérdida de la intgegridad o robo de información	4	3	6
			Entrenamiento insuficiente en seguridad	Error en el uso								
			Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos								
			Falta de autorización de los recursos de procesamiento de la información	Hurto de documentos								
			Falta de mecanismos de permisos para el acceso al documento									
A55	Aplicación Visual Fox Pro	Software	Defectos bien conocidos en el software	Abuso de los derechos	IDR126	Fallas en el proceso de definición de roles	Puestos de trabajo con accesos restringidos o amplios accesos	Uso inadecuado de los mismos	Debido a fallas en el proceso de definición de roles, algunos puestos de trabajo tengan accesos restringidos o amplios accesos, posibilitando el uso inadecuado de los mismos o limitando las funciones del puesto.	5	3	7
			Falta de pruebas de auditoría									

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Prob. Ocurr	Valor
A57	Paquetes de Cartas de Cobranza	Personal	Entrenamiento insuficiente en seguridad	Error en el uso	IDR127	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a información confidencial para el negocio , pudiendo afectar la integridad y/o disponibilidad de la información.	4	3	6
			Trabajo no supervisado del personal externo o de limpieza	Hurto de los paquetes								
			Falta de procedimientos para el manejo de información clasificada	Error en el uso								
			Falta de control de los activos que se encuentran fuera de las instalaciones	Hurto de los paquetes								
A48	Web Service	Software	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software	IDR128	Falla en el funcionamiento	Falla en los servicios	Pérdidas financieras / Incumplimiento de contrato	Debido al mal funcionamiento del sw, no se puedan realizar las actividades diarias (p.e. envío y recepción de solicitudes por por parte del cliente) generando improductividad en el negocio.	5	3	7
			Software nuevo o inmaduro									
			Falta o insuficiencia de la prueba del software	Abuso de los derechos	IDR129	Insuficientes pruebas	Accesos no autorizados	Pérdida de la integridad de la información / Robo de información	Acceso no autorizado pudiendo generar indisponibilidad del acceso a los aplicativos, pérdida de la integridad de la información	5	2	6
			Defectos bien conocidos en el software									
			Configuración incorrecta de parámetros	Error en el uso	IDR130	Falta de documentación	Procesamiento de data ilegal	Pérdidas financieras	Pérdida en la integridad de la información	5	2	6
			Falta de documentación									
			Habilitación de servicios innecesarios	Procesamiento ilegal de datos								
A17	Portal Web	Software	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos	IDR131	Fallas en el Sistema	Ingreso no Autorizado	Pérdida en la integridad de la Información	Personas no autorizadas ingresen al Portal, manipulándolo y causando pérdidas en la integridad de la información	5	3	7
			Distribución errada de los derechos de acceso									
			Interfase de usuario complicada	Error en el uso	IDR132	Errores en la asignación de perfiles	Inadecuada segregación de funciones	Controles sin efectividad	Debido a errores en la asignación de perfiles definidos para los roles del personal por tener una interfaz complicada para el Portal Web, no exista una adecuada segregación de funciones para los procesos de negocio, por lo que los controles de los procesos pierdan efectividad.	5	3	7
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos	IDR133	Inadecuadas políticas de almacenamiento de passwords	Contraseñas maestras accesadas por personal no autorizado	Inadecuados niveles de servicio y/o fuga de información	Debido a inadecuadas políticas de almacenamiento de passwords, las contraseñassean accesadas por personal no autorizado, pudiendo afectar los niveles de servicio y/o provocar fuga de información.	5	3	7
			Gestión deficiente de las contraseñas									
			Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR134	Actitud deshonesta del personal y/o proced. de baja de usuarios	Accesos a usuarios no autorizados	Robo y/o fuga de información	Debido a actitud deshonesta del personal, exista fraude interno al no realizar las bajas o cambios de roles oportunamente, generandose fuga y/o robo de información. O por no seguir un procedimiento formal se bloqueen los accesos a un usuario que cambia de puesto de trabajo.	5	3	7

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A58	Courier	Personal	Trabajo no supervisado de personal externo	Hurto de los documentos o paquetes	IDR135	Inadecuadas políticas de acceso y monitoreo	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso (por ejem: fallas en custodia de documentos) personal externo tenga acceso a equipos o documentación que almacenan o procesan información crítica para el negocio del Banco, pudiendo afectar la integridad y/o disponibilidad de la información.	4	3	6
			Falta de conciencia acerca de la seguridad	Error en el uso								
			Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con terceros	Abuso de los derechos								
			Falta de procedimientos para el manejo de información clasificada	Error en el uso								
			Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de activo								
A59	Cargo	Organización	Entrenamiento insuficiente en seguridad	Error en el uso	IDR136	Personal desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a que el personal (en especial los couriers) desconozcan las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	4	3	6
			Trabajo no supervisado del personal externo o de limpieza	Hurto de los paquetes								
			Falta de procedimientos para el manejo de información clasificada	Error en el uso								
			Falta de control de los activos que se encuentran fuera de las instalaciones	Hurto de los paquetes								
A60	Equipo móvil Nextel	Hardware	Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo. Polvo, corrosión, congelamiento	IDR137	Falta de capacitaciones	Falla en el servicio	Información no disponible / incumplimiento de contrato	Debido a falta de capacitaciones a empleados en seguridad y empleo de activos, se dañen o roben.	4	4	7
			Falta de cuidado en la disposición final	Hurto de equipo								
		Personal	Uso incorrecto de software y hardware	Error en el uso								
			Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A61	Aplicación B2B	Software	Defectos bien conocidos en el software	Abuso de los derechos	IDR138	Falta de pruebas	Falla en el servicio	Pérdidas financieras	Debido a fallas en la aplicación no se llegue a brindar el servicio	4	3	6
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos								
			Tablas de contraseñas sin protección									
A62	Servidor FTP	Hardware	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario cifrados	Falsificación de derechos	IDR139	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso personal no autorizado tenga acceso a pudiendo afectar la integridad y/o disponibilidad de la información.	4	4	7
				Corrupción de datos								
				Hurto de información								
A24	CD encriptado	Hardware	Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del CD Polvo, corrosión	IDR140	Inadecuadas políticas de almacenamiento	Información no disponible	Impacto en productividad del negocio, incumplimiento de contrato, incumplimiento de la ley	Por inadecuadas políticas de almacenamiento, se dañen CDs que almacenan información crítica para el negocio de la Central, pudiendo afectar la integridad y/o disponibilidad de la información.	4	3	6
			Almacenamiento sin protección	Hurto o destrucción de CD	IDR141	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a los Cds que almacenan información crítica para el negocio de la Central de Riesgo, pudiendo afectar la integridad y/o disponibilidad de la información o Robo	4	3	6
			Copia no controlada									
		Personal	Trabajo no supervisado del personal externo o de limpieza									

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A52	Personal de Tecnología como Servicio	Personal	Entrenamiento insuficiente en seguridad	Hurto de información	IDR142	Personal desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad / Robo de información / Divulgación / Pérdida de Integridad	Debido a que el personal de la Central desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	4	3	6
			Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo								
		Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR143	Falta de designación de owners	Se otorguen o eliminen accesos sin aprobaciones	Divulgación de información / pérdidas financieras	Debido a que no se cuenta con una relación de aplicativos (cliente/servidor y host) vs. owners, se otorguen o eliminen accesos sin contar con todas las aprobaciones requeridas, pudiendo facilitar la divulgación de información y el hurto de Información, ocasionando grandes pérdidas financieras	5	3	7
			Falta de proceso formal para la revisión (supervisión) de los derechos de acceso									
			Falta de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones								
			Falta de políticas sobre el uso del correo electrónico	Error en el uso								
			Falta de procedimientos para la introducción del software en los sistemas operativos									
			Falta de procedimientos para el manejo de información clasificada									
			Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos								
			Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo o información								
A78	Personal Servicio al Cliente	Personal	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo	IDR144	Actitud deshonesta del personal	Accesos inadecuados	Fuga y/o robo de información	Debido a actitud deshonesta del personal, exista fraude interno al no realizar las bajas o cambios de roles oportunamente, generandose fuga y/o robo de información.	5	3	7
			Ausencia del personal	Incumplimiento en la disponibilidad del personal								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A51	Personal de Tecnología de Información	Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal	IDR145	Inadecuados procesos de contrtación y falta de capacitación	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información / Pérdidas finacieras /Robo de información	Debido a que el personal desconozca las normas, políticas y criterios de seguridad de información, y en algunos casos debido a procedimientos inadecuados de contratación, se incumplan las normas internas pudiendo generar debilidades y vulnerabilidades de seguridad, errores en el uso de aplicativos, ypérdida de integridad de la información e incluso hurto y fraude.	5	4	8
			Procedimientos inadecuados de contratación	Destrucción de equipos o medios								
			Entrenamiento insuficiente en seguridad	Error en el uso								
			Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos								
			Trabajo no supervisado	Hurto de información o medios								
		Lugar	Falta de protección física de las puertas	Hurto de equipo	IDR146	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso físico, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio (medios de almacenamiento) pudiendo afectar la integridad y/o disponibilidad de la información.	5	4	8
		Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR147	Falta de segregación de funciones	Unidad sea responsable de definir/crear/aprobar cambios	Errores y/o abuso de funciones	Debido a falta de segregación de funciones, una misma unidad sea responsable de definir, crear y aprobar cambios en producción relacionado a roles, ocasionando errores y/o abuso de funciones.	5	4	8
			Falta de proceso formal para la revisión (supervisión) de los derechos de acceso									
			Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con terceros									
			Falta o insuficiencia en el acuerdo a nivel de servicio	Incumplimiento en el mantenimiento del sistema de información	IDR148	Falta de mantenimiento	Falla en los aplicativos	Acceso no autorizados, robo de información	Fallas en el funcionamiento de los aplicativos generando vulnerabildiades en la seguridad, accesos no autorizados, robo de información.	5	3	7
A26	Operadores	Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal	IDR149	Falta de disponibilidad de operadores	Operativa impactada de los procesos de negocio	Impacto en productividad del negocio	Debido a la falta de disponibilidad de operadores, haya un grave impacto en la productividad del negocio	5	3	7
			Procedimientos inadecuados de contratación	Destrucción de equipos o medios	IDR150	Desconocimiento de operadores de las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a que el personal desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	5	4	8
			Entrenamiento insuficiente en seguridad	Error en el uso de aplicaciones								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A26	Operadores	Organización	Falta de reportes sobre fallas incluidos en los registros de operadores	Abuso de los derechos	IDR153	Falta de registro de bitácoras e incidentes en seguridad	Operativa impactada de los procesos de negocio	Impacto en productividad del negocio	Debido a falta de procedimientos de registros de bitácora, no se puedan tomar acciones correctivas por tanto no se registren acciones correctivas alrededor de los incidentes en las actividades diarias	5	3	7
			Falta de registros en las bitácoras*(logs)	Error en el uso								
			Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos	IDR154	Actitud deshonesta del personal y falta de disposiciones en contratos	Fuga y/o robo de información	Pérdidas financieras / Incumplimiento de la ley	Debido a la falta de disposiciones en los contratos y a una actitud deshonesta del personal, exista fraude interno, generandose fuga y/o robo de información o pérdida de su integridad	5	3	7
A28	Servidores de Base de Datos	Hardware	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información	IDR155	Falta de mantenimiento	Acceso a la BD interrumpido	Operativa impactada de los procesos de negocio, improductivada d/ Pérdidas financieras	Debido a la falta de mantenimiento, el acceso a la Base de Datos se vea interrumpido	5	3	7
			Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento								
			Almacenamiento sin protección	Hurto de información	IDR156	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso (por ejem: fallas en custodia de archivos que contiene los passwords de los usuarios genéricos de aplicación del ambiente de producción,) personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio, pudiendo afectar la integridad y/o disponibilidad de la información.	5	2	6
			Uso inadecuado o descuidado del control de acceso físico a las edificaciones	Destrucción de equipo o medios								
			Copia no controlada	Hurto de información								
		Lugar	Falta de protección física de las puertas y ventanas de la edificación	Hurto de Servidor	IDR157	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio de la Central como los Servidores, pudiendo afectar la integridad y/o disponibilidad de la información.	5	2	6
A29	Servidores de Archivos	Hardware	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información	IDR158	Falta de mantenimiento	Acceso a la BD interrumpido	Operativa impactada de los procesos de negocio, improductivada d/ Pérdidas financieras	Debido a la falta de mantenimiento, el acceso a la Base de Datos se vea interrumpido	5	3	7
			Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento								
			Almacenamiento sin protección	Hurto de información	IDR159	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso personal no autorizado tenga acceso a servidores de archivos que contienen nformación crítica para el negocio, pudiendo afectar la integridad y/o disponibilidad de la información.	5	3	7
			Copia no controlada	Hurto de información								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A29	Servidores de Archivos	Lugar	Falta de protección física de las puertas y ventanas de la edificación	Hurto de Servidor	IDR 160	Inadecuados procedimientos de custodia	Acceso a personal no autorizado a equipos criticos	Indisponibilidad y/o falta de integridad de información	Debido a inadecuados procedimientos de custodia, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio de la Central, pudiendo afectar la disponibilidad e integridad de la información.	5	2	6
A29	Servidores de Archivos	Organización	Falta de autorización de los recursos de procesamiento de la información	Hurto de Servidor	IDR 160	Inadecuados procedimientos de custodia	Acceso a personal no autorizado a equipos criticos	Indisponibilidad y/o falta de integridad de información	Debido a inadecuados procedimientos de custodia, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio de la Central, pudiendo afectar la disponibilidad e integridad de la información.	5	2	6
			Falta de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo								
A16	Base de Datos Microsoft Sql Server 2003 - 2008	Software	Falta o insuficiencia de la prueba del software	Abuso de los derechos	IDR 161	Falta de logs	Intentos de acceso no autorizados	Ataques informáticos	Debido a insuficientes logs de auditoría, los intentos no autorizados de acceso a la Base de Datos no sean detectados y se produzcan ataques informáticos.	5	2	6
			Defectos bien conocidos en el software									
			Falta de pruebas de auditoría									
			Distribución errada de los derechos de acceso			Inadecuado procedimiento de identificación de funciones	Definición incorrecta de perfiles de acceso	Usuarios tengan accesos de más o restringidos	Debido a un inadecuado procedimiento de identificación de funciones, no se realice correctamente la definición de los perfiles de accesos y por ende los usuarios tengan accesos de más o restringidos.	4	2	5
A23	Personal Comercial - Ventas	Personal	Procedimientos inadecuados de contratación	Error en el uso de aplicativos	IDR 162	Incumplimiento de procedimientos	Ataques informaticos a aplicaciones del negocio	Indisponibilidad y/o falta de integridad de las aplicaciones	Por incumplimiento de procedimientos, se produzcan ataques informáticos a aplicaciones del negocio, o a equipos como servidores pudiendo provocar indisponibilidad y/o falta de integridad de las aplicaciones e información de Titulares	5	2	6
				Destrucción de equipos								
				Procesamiento ilegal de los datos								
		Organización	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR 163	Inadecuado procedimiento de baja de accesos	Falta de accesos	Improductividad	Debido a inadecuado procedimiento de baja de accesos, personal no pueda realizar sus labores por la falta de accesos a los diferentes sistemas, generando improductividad.	5	3	7
			Falta de proceso formal para la revisión (supervisión) de los derechos de acceso									
			Falta de procedimiento de monitoreo de los recursos de procesamiento información									
			Falta de políticas sobre el uso del correo electrónico	Error en el uso	IDR 164	Falta de políticas sobre el uso de correo electrónico	Ataques informáticos	Incumplimiento de la ley	Por falta de políticas para el uso del correo electrónico, se generen debilidades y vulnerabilidades de seguridad (ataques informáticos) y se divulgue información o se pierda la integridad de la misma	5	4	8
			Falta de procedimientos para la introducción del software en los sistemas operativos		IDR 165	Falta de procedimientos para la introducción de sw	Fuga y/o robo de información	Pérdidas financieras / Incumplimiento de la ley	Debido a la falta de procedimientos para la introducción de sw y una actitud deshonesta del personal de ventas, exista fraude interno, generandose fuga y/o robo de información.	5	3	7

7. Matriz de Riesgos: Comprar Información

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A65	Contrato (Fuentes)	Organización	Falta de revisiones en las disposiciones por parte de la gerencia	Usos no autorizados de hardware y software Hurto de equipos, documentos o/y información Abuso de los derechos	IDR292	Falta de revisión de contratos a personal y clientes	Fraude	Pérdida financiera	Debido a una falta de revisión de las disposiciones en los contratos con las fuentes, no se establezcan medidas de seguridad para con los clientes, generando fraudes ,y/o hurto de información o equipos sin la posibilidad de recibir una indemnización por la pérdida financiera generada	5	3	7
A67	Cintas magnéticas - Back ups	Hardware	Falta de esquemas de reemplazo periódico. Susceptibilidad a la humedad, el polvo y la suciedad. Almacenamiento sin protección Copia no controlada	Destrucción de los medios. Polvo, corrosión, congelamiento Hurto de medios	IDR293	Inadecuada gestión de accesos	Personal no autorizado acceda al centro de operaciones	Daño a equipos y/o robo de información	Debido a una inadecuada gestión de los accesos , personal no autorizado pueda acceder a las oficinas de Adquisición de Datos y pueda provocar daños a equipos y robo de medios de almacenamiento	4	4	7
A79	Personal Legal	Personal	Entrenamiento insuficiente en seguridad	Error en el uso de aplicaciones	IDR294	Incumplimiento de procedimientos	Ataques informaticos a aplicaciones del negocio	Indisponibilidad y/o falta de integridad de las aplicaciones	Por incumplimiento de procedimientos, se produzcan ataques informáticos a aplicaciones del negocio, o a equipos como servidores pudiendo provocar indisponibilidad y/o falta de integridad de las aplicaciones e información de Titulares	5	4	8
A80	Personal Adquisición de información	Personal	Entrenamiento insuficiente en seguridad Falta de mecanismos de monitoreo	Error en el uso de aplicaciones Procesamiento ilegal de los datos	IDR295	Personal desconozca las normas, políticas y criterios de seguridad	Incumplimiento de normas	Vulnerabilidad de seguridad	Debido a que el personal de limpieza de la Central desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	5	4	8

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A82	Personal Control de Calidad	Personal	Uso incorrecto de software y hardware	Error en el uso	IDR296	Personal no tenga el conocimiento suficinete para implementar y administrar la herramienta	Errores en el uso de aplicativos	Pérdida de integridad de la información	Debido a que personal no tenga el conocimiento suficiente para la utilización de aplicaciones o hw y a falta de monitorio, se presenten errores o ingreso ilegal de data.	4	3	6
A86	Puertas de entrada a las Oficinas	Lugar	Falta de protección física de las puertas, falta de mecanismode autentificación	Hurto de equipos o información	IDR297	Inadecuadas políticas de acceso al edificio	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Debido a inadecuadas políticas de seguridad para el acceso físico al edificio, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio del Banco, pudiendo afectar la integridad y/o disponibilidad de la información.	5	3	7
A24	CD encriptado	Hardware	Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del CD Polvo, corrosión	IDR298	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a los Cds que almacenan información crítica para el negocio de la Central de Riesgo, pudiendo afectar la integridad y/o disponibilidad de la información o Robo	5	3	7
			Almacenamiento sin protección	Hurto o destrucción de CD								
			Copia no controlada									
		Personal	Trabajo no supervisado del personal externo o de limpieza									
A48	Web Service	Software	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software	IDR299	Falla en el funcionamiento	Falla en los servicios	Pérdidas financieras / Incumplimiento de contrato	Debido al mal funcionamiento del sw, no se puedan realizar las actividades diarias (p.e. envío y recepción de solicitudes por por parte del cliente) generando improductividad en el negocio.	5	4	8
			Software nuevo o inmaduro									
			Falta o insuficiencia de la prueba del software	Abuso de los derechos	IDR300	Insuficientes pruebas	Accesos no autorizados	Pérdida de la integridad de la información / Robo de información	Acceso no autorizado pudiendo generar indisponibilidad del acceso a los aplicativos, pérdida de la integridad de la infrmación	5	4	8
			Defectos bien conocidos en el software									
			Configuración incorrecta de parámetros	Error en el uso	IDR301	Falta de documentación	Procesamiento de data ilegal	Pérdidas financieras	Pérdida en la itnegridad de la información	5	4	8
			Falta de documentación									
			Habilitación de servicios innecesarios	Procesamiento ilegal de datos								

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A17	Portal Web	Software	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo Distribución errada de los derechos de acceso	Abuso de los derechos	IDR302	Fallas en el Sistema	Ingreso no Autorizado	Pérdida en la integridad de la Información	Personas no autorizadas ingresen al Portal, manipulándolo y causando pérdidas en la integridad de la información	5	2	6
			Interfase de usuario complicada	Error en el uso	IDR303	Errores en la asignación de perfiles	Inadecuada segregación de funciones	Controles sin efectividad	Debido a errores en la asignación de perfiles definidos para los roles del personal por tener una interfaz complicada para el Portal Web, no exista una adecuada segregación de funciones para los procesos de negocio, por lo que los controles de los procesos pierdan efectividad.	5	3	7
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario Gestión deficiente de las contraseñas	Falsificación de derechos	IDR304	Inadecuadas políticas de almacenamiento de passwords	Contraseñas maestras accesadas por personal no autorizado	Inadecuados niveles de servicio y/o fuga de información	Debido a inadecuadas políticas de almacenamiento de passwords, las contraseñassean accesadas por personal no autorizado, pudiendo afectar los niveles de servicio y/o provocar fuga de información.	5	3	7
			Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR305	Actitud deshonesta del personal y/o falta de procedimiento de baja de usuarios	Accesos a usuarios no autorizados	Robo y/o fuga de información	Debido a actitud deshonesta del personal, exista fraude interno al no realizar las bajas o cambios de roles oportunamente, generandose fuga y/o robo de información. O por no seguir un procedimiento formal se bloqueen los accesos a un usuario que cambia de puesto de trabajo.	5	3	7
A70	Datamart	Software	Falta de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos	IDR306	Inadecuados procesos de detección	Intentos no autorizados de acceso a información	Error en los mecanismos de detección de ataques internos/externos / Pérdidas financieras	Debido a inadecuados procesos de detección, los intentos no autorizados de acceso a información del Datamart no sean detectados y se produzcan ataques informáticos	5	3	7
			Falta de copias de respaldo	Manipulación con software								
A71	Host	Hardware	Falta de planes de continuidad	Fallas en equipo . Abuso de los derechos	IDR307	Inadecuados procedimientos de custodia	Acceso a personal no autorizado a equipos criticos	Indisponibilidad y/o falta de integridad de información	Debido a inadecuados procedimientos de custodia, personal no autorizado tenga acceso al Host, el cual procesa toda la información crítica del negocio, impactando gravemente en la disponibilidad, confidencialidad e integridad de la información.	5	2	6
			Falta de procedimiento de monitoreo									
			Falta de procedimientos de identificación y evaluación de riesgos									
			Falta de reportes sobre fallas		IDR308	Inadecuada gestión de accesos	Personal no autorizado acceda al CC	Daño a equipos y/o robo de información	Debido a una inadecuada gestión de los accesos en el centro de cómputo, personal no autorizado pueda acceder, pudiendo provocar daños a equipos y/o robo de información.	5	2	6

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A76	Documento Word de la cotización	Software	Falta de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos	IDR309	Falta de políticas de otorgamiento de accesos	Acceso no autorizado	Pérdida de integridad / Robo	Debido a una inadecuada gestión de accesos, se otorguen mayores accesos a los usuarios de los que se definieron inicialmente o accesos a usuarios no autorizados , posibilitando la pérdida de integridad de la información o robo de información debido al interés de la competencia.	5	3	7
			Trabajo no supervisado del personal externo o de limpieza	Hurto de infomación								
			Falta de mecanismos de permisos para el acceso al documento									
A81	Personal Operaciones	Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal	IDR310	Incumplimiento de procedimientos	Ataques informaticos a aplicaciones del negocio	Indisponibilidad y/o falta de integridad de las aplicaciones	Por procedimientos inadecuados de contratación y falta de mecanismos de monitorei, se produzcan ataques informáticos a aplicaciones del negocio, o a equipos como servidores pudiendo provocar indisponibilidad y/o falta de integridad de las aplicaciones e información de Titulares	5	3	7
			Procedimientos inadecuados de contratación	Destrucción de equipos o medios								
			Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos								
A66	Aplicación Visual Fox Pro / BD	Software	Falta o insuficiencia de la prueba del software	Abuso de los derechos	IDR311	Fallas en el proceso de definición de roles	Puestos de trabajo con accesos restringidos o amplios accesos	Uso inadecuado de los mismos	Debido a fallas en el proceso de definición de roles, algunos puestos de trabajo tengan accesos restringidos o amplios accesos, posibilitando el uso inadecuado de los mismos o limitando las funciones del puesto.	5	3	7
			Defectos bien conocidos en el software									
			Falta de pruebas de auditoría									
			Distribución errada de los derechos de acceso									
A16	Base de Datos Microsoft Sql Server 2003 - 2008	Software	Falta o insuficiencia de la prueba del software	Abuso de los derechos	IDR312	Falta de logs	Intentos de acceso no autorizados	Ataques informáticos	Debido a insuficientes logs de auditoría, los intentos no autorizados de acceso a la Base de Datos no sean detectados y se produzcan ataques informáticos.	5	4	8
			Defectos bien conocidos en el software									
			Falta de pruebas de auditoría									
			Distribución errada de los derechos de acceso		IDR313	Inadecuado procedimiento de identificación de funciones	Definición incorrecta de perfiles de acceso	Usuarios tengan accesos de más o restringidos	Debido a un inadecuado procedimiento de identificación de funciones, no se realice correctamente la definición de los perfiles de accesos y por ende los usuarios tengan accesos de más o restringidos.	5	4	8

ID	Activo	Tipo de Vulnerabilidad	Vulnerabilidad	Amenaza	IDR	Causa	Evento	Consecuencia	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor
A28	Servidores de Base de Datos	Hardware	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información	IDR314	Falta de mantenimiento	Acceso a la BD interrumpido	Operativa impactada de los procesos de negocio, improductividad/ Pérdidas financieras	Debido a la falta de mantenimiento, el acceso a la Base de Datos se vea interrumpido	5	3	7
			Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento								
			Almacenamiento sin protección	Hurto de información	IDR315	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso (por ejem: fallas en custodia de archivos que contiene los passwords de los usuarios genéricos de aplicación del ambiente de producción,) personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio, pudiendo afectar la integridad y/o disponibilidad de la información.	5	4	8
			Uso inadecuado o descuidado del control de acceso físico a las edificaciones	Destrucción de equipo o medios								
			Copia no controlada	Hurto de información								
		Lugar	Falta de protección física de las puertas y ventanas de la edificación	Hurto de Servidor	IDR316	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio de la Central como los Servidores, pudiendo afectar la integridad y/o disponibilidad de la información.	5	2	6
A29	Servidores de Archivos	Hardware	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información	IDR317	Falta de mantenimiento	Acceso a la BD interrumpido	Operativa impactada de los procesos de negocio, improductividad/ Pérdidas financieras	Debido a la falta de mantenimiento, el acceso a la Base de Datos se vea interrumpido	5	2	6
			Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento								
			Almacenamiento sin protección	Hurto de información	IDR318	Inadecuadas políticas de acceso	Personal no autorizado tenga acceso a información confidencial	Falta de integridad y/o disponibilidad de la información	Por inadecuadas políticas de acceso personal no autorizado tenga acceso a servidores de archivos que contienen nformación crítica para el negocio, pudiendo afectar la integridad y/o disponibilidad de la información.	4	3	6
			Copia no controlada	Hurto de información								
		Lugar	Falta de protección física de las puertas y ventanas de la edificación	Hurto de Servidor	IDR319	Inadecuados procedimientos de custodia	Acceso a personal no autorizado a equipos criticos	Indisponibilidad y/o falta de integridad de información	Debido a inadecuados procedimientos de custodia, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio de la Central, pudiendo afectar la disponibilidad e integridad de la información.	5	3	7
			Ubicación en un área susceptible de inundación	Inundación								
		Organización	Falta de autorización de los recursos de procesamiento de la información	Hurto de Servidor								
			Falta de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo								

Anexo 4

Tratamiento de Riesgos – Declaración de la Aplicabilidad

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A01	Generar Reporte Crediticio por Agencia	Representates de Servicio al Cliente (RSC)	Entrenamiento insuficiente en seguridad	Uso no autorizado de equipo	IDR04	Personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio de la Central, pudiendo afectar la disponibilidad e integridad de la información.	5	2	6	7.2.2	Procedimientos de manipulación de la información: Los procedimientos para la manipulación y almacenamiento de la información deben ser establecidos para proteger esta información de divulgaciones o usos no autorizados. Restricciones de acceso para identificar al personal no autorizado.	La Central de Riesgo debe definir un procedimiento claro para el manejo de sus activos de información durante sus procesos y de esta forma asegurar que esten protegidos y evitar el aceso de peronas no autorizadas a estos.	Sí	La Central de Riesgo deberá analizar los procesos afectados y de esta manera corregir las deficiencias encontradas (ausencia de personal) que podrían acpntecer con incidencias de seguridad.
			Uso incorrecto de software y hardware	Error en el uso	IDR05	Debido a insuficientes políticas de protección y falta de capacitación, los equipos se encuentren desprotegidos y se exploten vulnerabilidades, pudiendo afectar afectar la disponibilidad e integridad de la información.	5	3	7					
			Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo	IDR06	Por falta de políticas del uso de correo electrónico, se produzcan ataques informáticos a aplicaciones del negocio, pudiendo provocar indisponibilidad y/o falta de integridad de las aplicaciones.	5	4	8					
			Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR07	Por inadecuadas políticas de registro y retiro de registro de usuario, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio de la Central, pudiendo afectar la integridad y/o disponibilidad de la información.	5	3	7					

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A02	Generar Reporte Crediticio por Agencia / Generar Venta por Web / Generar Venta de Servicios Complementarios	Aplicación Web Reporte Crediticio Online	El aplicativo web contiene defectos o fallas en su desarrollo.	Mal funcionamiento del software	IDR08	Debido a un mal funcionamiento de algunos aplicativos web podrían haber intentos no autorizados de acceso que no sean detectados y se produzcan ataques informáticos, lo que conlleva a robo o fuga de información	5	3	7	9.4.1	Sesiones inactivas deben cerrar después de un período definido de inactividad.	Las sesiones a los sistemas y conexiones de red de la Central deberán ser finalizadas luego de un periodo definido d e inactividad.	Sí	Al igual que las sesiones de sistema, las sesiones activas a las distintas aplicaciones del Central de Riesgo deberán ser finalizadas luego de un periodo definido de tiempo. Esto se puede lograr estableciendo dichas condiciones en los aplicativos que son mantenidos por el Central de Riesgo, de manera que pueda establecerse la finalización de la sesión en cada aplicativo.
			Falta de mecanismos de autenticación e identificación de usuario	Falsificación de derechos	IDR11	Debido a la falta de mecanismos de autenticación e identificación de usuarios / logs insuficientes, no sea posible identificar a usuario y por ende no sea posible tomar acción correctiva.	5	2	6	9.4.2	Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal, y una técnica de autenticación adecuado debe ser elegido para demostrar la identidad alegada de un usuario.	La Central de Riesgo debe controlar la asignación de contraseñas mediante un proceso formal en el cual designe la responsabilidad sobre estas a los dueños de las mismas.	Sí	La Central de Riesgo deberá mejorar la forma en la que asigna ya la asignación de contraseñas y no dejar relegada esta gestión ya que depende de ella se otorgan accesos a la información. Para el caso, será necesario establecer registros en los cuales se cuente con la identificación de usuarios y sus respectivas contraseñas.
			Interfaz de usuario complicada	Error en el uso	IDR12	Debido a una interfaz complicada, no se realice correctamente la definición de los perfiles de accesos y por ende los usuarios tengan accesos de más o restringidos.	4	3	6	9.4.4	El acceso a la información y funciones de la aplicación del sistema por los usuarios y personal de apoyo deben limitarse de acuerdo con la política de control de acceso definidas.	La Central de Riesgo debe definir un procedimiento claro para el manejo de sus activos de información durante sus procesos y de esta forma asegurar que esten protegidos y evitar el acceso de peronas no autorizadas a estos.	Sí	La Central de Riesgo deberá analizar los procesos afectados y de esta manera corregir las deficiencias encontradas (ausencia de personal) que podrían acpntecer con incidencias de seguridad.
			Faltas de las pruebas de software	Abuso de derechos	IDR13	Debido a la falta de pruebas en el software traiga como consecuencia una inadecuada gestión de accesos y se otorguen mayores accesos a los usuarios de los que se definieron inicialmente, posibilitando el uso incorrecto de los mismos.	4	3	6					

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A02	Generar Reporte Crediticio por Agencia / Generar Venta por Web / Generar Venta de Servicios Complementarios	Aplicación Web Reporte Crediticio Online	Falta de documentación y actualización de dicha documentación	Error en el uso	IDR14	Por falta de documentación (manuales, procedimientos, reporte de turnos e indicadores de gestión), haya la posibilidad de fallas en el otorgamiento de accesos generando fuga de información	4	4	7	12.1.1	El acceso a la información y funciones de la aplicación del sistema por los usuarios y personal de apoyo deben limitarse de acuerdo con la política de control de acceso definidas.	La Central de Riesgo debe definir un procedimiento claro para el manejo de sus activos de información durante sus procesos y de esta forma asegurar que esten protegidos y evitar el aceso de peronas no autorizadas a estos.	Sí	La Central de Riesgo deberá analizar los procesos afectados y de esta manera corregir las deficiencias encontradas (ausencia de personal) que podrían acpntecer con incidencias de seguridad.
			Gestión deficiente de las contraseñas	Falsificación de derechos	IDR15	Debido a inadecuadas políticas de almacenamiento de passwords, las contraseñas maestras sean accesadas por personal no autorizado, pudiendo afectar los niveles de servicio y/o provocar fuga de información.	5	4	8	9.4.3	Gestión de contraseñas de usuario: Se debería controlar la asignación de contraseñas por medio de un proceso de gestión formal. a) requerir que los usuarios firmen un compromiso para mantener en secreto sus contraseñas personales y las compartidas por un grupo sólo entre los miembros de ese grupo.	La Central debe controlar la asignación de contraseñas mediante un proceso formal en el cual designe la responsabilidad sobre estas a los dueños de las mismas.	Sí	La Central de Riesgo deberá mejorar la forma en la que realiza la asignación de contraseñas y no dejar relegada esta gestión ya que depende de ella se otorgan accesos a la información. Para el caso, será necesario establecer registros en los cuales se cuente con la identificación de usuarios y sus respectivas contraseñas.
			Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de derechos	IDR18	Debido a errores en el procedimiento de baja de usuarios, no se dé de baja o bloquee los accesos a un usuario que cambia de puesto de trabajo, posibilitando el robo y/o fuga de información.	5	4	8	9.4.1	La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares a través de un proceso formal.	Los empleados del Central de Riesgo deberán ejercer la terminación de las sesiones activas antes de marcharse.	Sí	Este control puede implementarse educando al empleado o estableciendo parámetros en el dominio con el que cuenta el Central de Riesgo de manera que se pueda cumplir con la terminación de sesiones activas luego de cierto tiempo.

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A03	Generar Reporte Crediticio por Agencia / Generar Venta de Servicios Complementarios	PCs	Falta o insuficiencia en el acuerdo a nivel de servicio	Incumplimiento en el mantenimiento de los sistemas de información	IDR19	Falla en el funcionamiento de los aplicativos debido al incumplimiento del mantenimiento de la PC lo que podría generar un impacto en la productividad del negocio	5	3	7	11.2.7	Un proceso de autorización de la administración para las nuevas instalaciones de procesamiento de información deben ser definidas e implementadas.	El Central de Riesgo deberá otorgar accesos a el personal que lo necesite, restringiendo las funciones de sistema que no sean necesarias para cada empleado.	Sí	El Central de Riesgo deberá establecer las restricción en base a perfiles que se les dará a sus empleados de manera que tengan sólo acceso a las funciones necesarias para ellos. Esto se logrará a medida que se logre implantar en cada sistema.
			Susceptibilidad al polvo, suciedad	Corrosión, destrucción del equipo						11.2.6	Los usuarios deben asegurarse de que el equipo desatendido tiene la protección adecuada.	Los empleados del Central de Riesgo deberán ejercer la terminación de las sesiones activas antes de marcharse.	Sí	Este control puede implementarse educando al empleado o estableciendo parámetros en el dominio con el que cuenta el Central de Riesgo de manera que se pueda cumplir con la terminación de sesiones activas luego de cierto tiempo.
A04	Generar Reporte Crediticio por Agencia	Reporte Crediticio	Entrenamiento insuficiente en seguridad	Errores en el uso de aplicaciones o en el proceso	IDR20	Debido a falta de capacitación en seguridad, los empleados incumplan con la confidencialidad de la información del Titular pudiendo divulgarla.	5	4	8	7.1.2	Todos los activos deben estar claramente identificados y un inventario de todos los activos importantes elaborado y mantenido.	El Central de Riesgo deberá establecer una clasificación para la información y su asociación con las instalaciones de precesamiento de información.	Sí	Actualmente el Central de Riesgo cuenta con algunas tipificaciones de información. Debe establecer una clasificación para la inormación de manera que sea valida para toda la organización y de esta forma poder respetar la clasificación en cada instalción que esta sea procesada.
			Falta de conciencia acerca de la seguridad	Error en el uso del Reporte Crediticio										
			Trabajo no supervisado del personal externo o de limpieza	Hurto de documentos (Reporte Crediticio)	IDR21	Debido a actitud deshonesta del personal, exista robo de documentación (Reportes) , generandose fuga y atentado contra la confidencialidad del Titular.	5	3	7					

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A07	Generar Reporte Crediticio por Agencia / Generar Venta de Servicios Complementarios	Aplicación Ventas	Gestión deficiente de las contraseñas	Falsificación de derechos	IDR24	Debido a inadecuadas políticas de almacenamiento de passwords, las contraseñas al Módulo de Ventas sean accesadas por personal no autorizado, pudiendo provocar fuga de información y grandes pérdidas financieras	5	3	7	9.4.3	Información involucrada en las transacciones en línea debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración mensaje no autorizada, revelación no autorizada, mensaje no autorizado, duplicación o repetición.	El Central de Riesgo deberá otorgar accesos a el personal que lo necesite, restringiendo las funciones de sistema que no sean necesarias para cada empleado.	Sí	El Central de Riesgo deberá establecer las restricción en base a perfiles que se les dará a sus empleados de manera que tengan sólo acceso a las funciones necesarias para ellos. Esto se logrará a medida que se logre implantar en cada sistema.
			Falta de control eficaz del cambio	Mal funcionamiento del software	IDR25	Por falta de respaldo o un control eficaz del software, se afecte la operativa de los procesos de negocio soportados y por ende la productividad del negocio.	4	3	6	14.2.2	Sesiones inactivas deben cerrar después de un período definido de inactividad.			
			Falta de copias de respaldo	Manipulación del software										
A10	Generar Reporte Crediticio por Agencia / Generar Venta de Servicios Complementarios	Manual de Uso de Aplicación Web del Reporte Crediticio	Falta de políticas para la utilización de activos de la empresa	Error en el uso	IDR27	Por fallas en la gestión (almacenamiento) de la documentación (manuales, procedimientos, reporte de turnos e indicadores de gestión), esta no se encuentre disponible o pueda ser accedido por personal no autorizado, facilitando su copia a hurto	4	4	7	12.1.1	Todos los activos deben estar claramente identificados y un inventario de todos los activos importantes elaborado y mantenido.	El Central de Riesgo deberá establecer una clasificación para la información y su asociación con las instalaciones de precesamiento de información.	Sí	Actualmente el Central de Riesgo cuenta con algunas tipificaciones de información. Debe establecer una clasificación para la inormación de manera que sea valida para toda la organización y de esta forma poder respetar la clasificación en cada instalción que esta sea procesada.
				Hurto del manual o copias ilegales										

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A10	Generar Reporte Crediticio por Agencia / Generar Venta de Servicios Complementarios	Manual de Uso de Aplicación Web del Reporte Crediticio	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Copiado del software o el manual	IDR27	Por fallas en la gestión (almacenamiento) de la documentación (manuales, procedimientos, reporte de turnos e indicadores de gestión), esta no se encuentre disponible o pueda ser accedido por personal no autorizado, facilitando su copia a hurto	4	4	7	12.1.1	Todos los activos deben estar claramente identificados y un inventario de todos los activos importantes elaborado y mantenido.	El Central de Riesgo deberá establecer una clasificación para la información y su asociación con las instalaciones de precesamiento de información.	Sí	Actualmente el Central de Riesgo cuenta con algunas tipificaciones de información. Debe establecer una clasificación para la inormación de manera que sea valida para toda la organización y de esta forma poder respetar la clasificación en cada instalción que esta sea procesada.
A14	Generar Reporte Crediticio por Agencia / Generar Venta de Servicios Complementarios	Antivirus McAffe	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Mal funcionamiento del software Falsificación de derechos Uso de software falso o copiado Abuso de derechos	IDR29	Debido al uso de un software pirata, un virus y/o ataque informático genere bloqueo masivo de cuentas, generando indisponibilidad de usuarios y/o aplicaciones y pérdidas financieras	5	2	6	12.2.1	Los controles de detección, prevención y recuperación para proteger contra código malicioso y los procedimientos adecuados de sensibilización de los usuarios deben ser implementadas.	Se deberán elaborar guías de clasificación de la información en base a distintos aspectos de manera que se pueda asegurar la pretección de la misma.	Sí	Actualmente el Central de Riesgo cuenta con algunas tipificaciones de información. Debe establecer una clasificación para la inormación de manera que sea valida para toda la organización y de esta forma poder respetar la clasificación en cada instalción que esta sea procesada.

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
			Falta de políticas de seguridad de Firewalls	Uso no autorizado del equipo	IDR30	Debido a que no se tengan establecidas políticas de Seguridad para accesos a la red a través de Firewalls, se aperturen puertos abriendo nuevas vulnerabilidades y posibilidades de ataque informático.	5	3	7	13.1.1	Los controles de detección, prevención y recuperación para proteger contra código malicioso y los procedimientos adecuados de sensibilización de los usuarios deben ser implementadas.	Se deberán elaborar guías de clasificación de la información en base a distintos aspectos de manera que se pueda asegurar la pretección de la misma.	Sí	Actualmente el Central de Riesgo cuenta con algunas tipificaciones de información. Debe establecer una clasificación para la inormación de manera que sea valida para toda la organización y de esta forma poder respetar la clasificación en cada instalción que esta sea procesada.
				Abuso de derechos	IDR31	Debido a incumplimiento de políticas de seguridad de firewall, se instale un equipo Firewall sin proteccion, exponiendo a ataques a los servidores.	5	4	8					
A16	Generar Reporte Crediticio por Agencia / Generar Venta por Web / GGenerar Servicios Etapa Prospección	Base de Datos	Falta o insuficiencia de la prueba del software Defectos bien conocidos en el software Falta de pruebas de auditoría Distribución errada de los derechos de acceso	Abuso de los derechos	IDR33	Debido a insuficientes logs de auditoría, los intentos no autorizados de acceso a la Base de Datos no sean detectados y se produzcan ataques informáticos.	5	2	6	12.4.3	Auditoría registra las actividades de registro de usuarios, excepciones y eventos de seguridad de la información deben ser producidos y mantenidos por un período acordado para ayudar en futuras investigaciones y el monitoreo de control de acceso.	El Central de Riesgo debe establecer un mecanismo (cámaras de vigilancia) con el cual sea capaz de mantener un registro de las acciones realizadas por sus empleadores y/o personas que se encuentran en las instalaciones de la organización con el fin de asegurar un monitereo a sobre los activos de información de la organización.	Sí	La organización cuenta actualmente con un sector de las instalaciones monitoreado por un pequeño circuito de cámaras de vigilancia. Debería expandir este mecanismo al resto de sectores para de esta manera poder monitorear las actividades que realizan sus empleados y también porder seguir de cerca las incidencias que podrían darse con los activos de información en este caso con los documentos de traducción que se alamacenan y los exámenes de clasificación.

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A40	Generar Reporte Crediticio por Agencia / Generar Venta de Servicios Complementarios	Personal Contabilidad	Procedimientos inadecuados de contratación	Destrucción de equipos o medios	IDR34	Debido a que el personal desconozca las normas, políticas y criterios de seguridad de información, y en algunos casos debido a procedimientos inadecuados de contratación, se incumplan las normas internas pudiendo generar debilidades y vulnerabilidades de seguridad, errores en el uso de aplicativos y pérdida de integridad de la información	5	3	7	7.1.1	Una política de control de acceso debe ser establecida, documentada y revisada sobre la base de los negocios y los requisitos de seguridad para el acceso.	El Central de Riesgo deberá establecer una clasificación para la información y su asociación con las instalaciones de precesamiento de información.	Sí	Actualmente el Central de Riesgo cuenta con algunas tipificaciones de información. Debe establecer una clasificación para la inormación de manera que sea valida para toda la organización y de esta forma poder respetar la clasificación en cada instalción que esta sea procesada.
			Uso incorrecto de software y hardware	Error en el uso										
			Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos										
			Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo										
A13	Generar Reporte Crediticio por Agencia / Generar Venta de Servicios Complementarios	Personal de soporte	Ausencia del personal	Incumplimiento en la disponibilidad del personal	IDR35	Debido a actitud deshonesta del personal, exista fraude interno generándose fuga y/o robo de información.	4	4	7	7.1.2	La asignación y uso de privilegios debe ser restringido y controlado.	El Central de Riesgo debe establecer un procedimiento formal de intercambio de información que con el fin de proteger la información durante el intercambio de la misma.	Sí	El centro debería tener identificada la información en todo momento y saber donde se encuentra y quien accede a esta. Para este caso se encontró que las fchas con el nivel del alumno están expuestas a modificaciones y por ende podrían ser ingresadas como data corrupta al sistema. Por estos motivos se debe establecer el procedimiento de intercambio de información durante este proceso de manera que se evite estás exposiciones inseguras.
			Falta de conciencia acerca de la seguridad	Error en el uso										
			Falta de políticas para el uso de correo electrónico	Uso no autorizado del equipo										
			Falta de disposiciones (con respecto a la seguridad) en los contratos con terceros	Abuso de los derechos	IDR36	Por incumplimiento de procedimientos, se produzcan ataques informáticos a aplicaciones del negocio, pudiendo provocar indisponibilidad y/o falta de integridad de las aplicaciones.	5	4	8					

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A13	Generar Reporte Crediticio por Agencia / Generar Venta de Servicios Complementarios	Personal de soporte	Falta de procedimiento de monitoreo de los recursos de procesamiento información	Abuso de los derechos	IDR36	Por incumplimiento de procedimientos, se produzcan ataques informáticos a aplicaciones del negocio, pudiendo provocar indisponibilidad y/o falta de integridad de las aplicaciones.	5	4	8	7.2.2	La asignación y uso de privilegios debe ser restringido y controlado.	La Central de Riesgo debe establecer un procedimiento formal de intercambio de información que con el fin de proteger la información durante el intercambio de la misma.	Sí	La central debería tener identificada la información en todo momento y saber donde se encuentra y quien accede a esta. Para este caso se encontró que las fchas con el nivel del alumno están expuestas a modificaciones y por ende podrían ser ingresadas como data corrupta al sistema. Por estos motivos se debe establecer el procedimiento de intercambio de información durante este proceso de manera que se evite estás exposiciones inseguras.
			Falta de reportes sobre fallas incluidos en los registros de administradores y operador	Abuso de los derechos										
			Falta de procedimientos para la introducción del software en los sistemas operativos	Error en el uso	IDR37	Instalación de aplicativos de fuente desconocida pudiendo conllevar a ataques informáticos y causando desprestigio a la empresa por la divulgación de la información	5	4	8					
A37	Generar Reporte Crediticio por Agencia	Oficina Agencia	Uso inadecuado o descuidado del control de acceso físico	Destrucción de equipo o medios	IDR38	Debido a la falta de seguridad y vigilancia en la entrada de la Agencia pueda efectuarse un robo, daño de equipos o de información afectando la confidencialidad del Titular y pérdidas financieras para la Organización	5	2	6	11.1.1	Perímetros de seguridad (barreras, como paredes, puertas de entrada de tarjetas de control con dotación o escritorios de recepción) se debe utilizar para proteger áreas que contienen información y las instalaciones de procesamiento de información.	La Central de Riesgo deberá minimalizar las indicaciones del propósito de sus oficinas, sin signos obvios, fuera o dentro del edificio, que identifiquen la presencia de actividades de tratamiento de información en ellas.	Sí	Se deberá evaluar todas la simbología establecida en las instalaciones y distintas sedes del Central de Riesgo a medida que se determine el propósito de cada símbolo y se pueda retirar lo que sea inadecuado.
			Falta de protección física de las puertas y ventanas de la edificación	Hurto de equipo										

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A39	Generar Reporte Crediticio por Agencia / Generar Venta de Servicios Complementarios	Personal de Mantenimiento (Limpieza)	Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos conterceras partes	Abuso de los derechos	IDR39	Debido a que el personal de limpieza de la Central desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	5	4	8	5.1.2 6.1.1	Una política de escritorio limpio de papeles y soportes de almacenamiento extraíbles y una política clara pantalla para las instalaciones de procesamiento de la información debe ser adoptada.	Las computadoras del Central de Riesgo deberán ser protegidas con un mecanismo de protección de pantalla o de teclado controlado por contraseña u otro mecanismo de autentificación.	Sí	Este control puede implementarse educando al empleado o estableciendo parámetros en el dominio con el que cuenta el Central de Riesgo de manera que se pueda cumplir con la terminación de sesiones activas luego de cierto tiempo.
			Falta o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos	IDR40									
			Entrenamiento insuficiente en seguridad	Error en el uso	IDR41									
			Trabajo no supervisado del personal de limpieza	Hurto de medios o documentos	IDR42	Debido a inadecuados procedimientos de custodia, personal de limpieza tenga acceso a equipos que almacenan o procesan información crítica para el negocio de la central, pudiendo afectar la disponibilidad e integridad de la información.	5	3	7	5.1.2	La política de seguridad de la información debe ser revisado a intervalos planeados o si ocurren cambios significativos para asegurarse de su conveniencia, adecuación y eficacia.	La Central de Riesgo deberá otorgar accesos a el personal que lo necesite, restringiendo las funciones de sistema que no sean necesarias para cada empleado.	Sí	Lal Central de Riesgo deberá establecer las restricción en base a perfiles que se les dará a sus empleados de manera que tengan sólo acceso a las funciones necesarias para ellos. Esto se logrará a medida que se logre implantar en cada sistema.

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A17	Generar Venta por Web / Generar Venta de Servicios Complementarios / Generar Servicios Etapa Prospección	Portal Web	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo Distribución errada de los derechos de acceso	Abuso de los derechos	IDR43	Personas no autorizadas ingresen al Portal, manipulándolo y causando pérdidas en la integridad de la información	5	2	6	9.4.1	Información involucrada en el comercio electrónico que pasa a través de redes públicas deben ser protegida de actividad fraudulenta, disputa contractual, y la divulgación no autorizada o modificación	El Central de Riesgo debe establecer un procedimiento formal de intercambio de información que con el fin de proteger la información durante el intercambio de la misma.	Sí	El centro debería tener identificada la información en todo momento y saber donde se encuentra y quien accede a esta. Para este caso se encontró que las fchas con el nivel del alumno están expuestas a modificaciones y por ende podrían ser ingresadas como data corrupta al sistema. Por estos motivos se debe establecer el procedimiento de intercambio de información durante este proceso de manera que se evite estás exposiciones inseguras.
			Interfaz de usuario complicada	Error en el uso	IDR44	Debido a errores en la asignación de perfiles definidos para los roles del personal por tener una interfaz complicada para el Portal Web, no exista una adecuada segregación de funciones para los procesos de negocio, por lo que los controles de los procesos pierdan efectividad.	5	3	7					
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario Gestión deficiente de las contraseñas	Falsificación de derechos	IDR45	Debido a inadecuadas políticas de almacenamiento de passwords, las contraseñassean accesadas por personal no autorizado, pudiendo afectar los niveles de servicio y/o provocar fuga de información.	5	3	7					

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A17	Generar Venta por Web / Generar Venta de Servicios Complementarios / Generar Servicios Etapa Prospección	Portal Web	Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR46	Debido a actitud deshonesta del personal, exista fraude interno al no realizar las bajas o cambios de roles oportunamente, generandose fuga y/o robo de información. O por no seguir un procedimiento formal se bloqueen los accesos a un usuario que cambia de puesto de trabajo.	5	3	7	9.4.5	Información involucrada en las transacciones en línea debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración mensaje no autorizada, revelación no autorizada, mensaje no autorizado, duplicación o repetición.	El Central de Riesgo debe definir un procedimiento claro para el manejo de sus activos de información durante sus procesos y de esta forma asegurar que esten protegidos y evitar el aceso de peronas no autorizadas a estos.	Sí	El centro debería tener identificada la información en todo momento y saber donde se encuentra y quien accede a esta. Para este caso se encontró que las fchas con el nivel del alumno están expuestas a modificaciones y por ende podrían ser ingresadas como data corrupta al sistema. Por estos motivos se debe establecer el procedimiento de intercambio de información durante este proceso de manera que se evite estás exposiciones inseguras.
A28	Generar Venta por Web / Generar Venta de Servicios Complementarios	Servidores de Base de Datos	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información	IDR48	Debido a la falta de mantenimiento, el acceso a la Base de Datos se vea interrumpido	5	2	6	11.2.4	Normas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de información deben ser identificados, documentados e implementados.	El Central de Riesgo deberá encargarse de mantener adecuadamente los equipos de acuerdo a las indicaciones de los proveedores para asegurar su continua disponibilidad e integridad.	Sí	El Central de Riesgo deberá seguir lo detallado en los manuales de los equipos para poder cumplir con el mantenimiento de los mismos y esporádicamente contratar servicios de mantenimiento siempre y cuando sea necesario.
			Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento										
			Almacenamiento sin protección	Hurto de información	IDR49	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a Servidores que almacenan o procesan información crítica para el negocio de la Central, pudiendo afectar la integridad y/o disponibilidad de la información.	5	2	6					
			Uso inadecuado o descuidado del control de acceso físico a las edificaciones	Destrucción de equipo o medios										
			Copia no controlada	Hurto de información	IDR50	Debido a inadecuado procedimiento de custodia de información confidencial, la Base de datos sea accesada por personal no autorizado con posible riesgo de acceso y/o divulgación de información.	5	3	7					

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A28	Generar Venta por Web / Generar Venta de Servicios Complementarios	Servidores de Base de Datos	Falta de protección física de las puertas y ventanas de la edificación	Hurto de Servidor	IDR51	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio de la Central como los Servidores, pudiendo afectar la integridad y/o disponibilidad de la información.	5	3	7	11.2.5	Normas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de información deben ser identificados, documentados e implementados.	El Central de Riesgo deberá encargarse de mantener adecuadamente los equipos de acuerdo a las indicaciones de los proveedores para asegurar su continua disponibilidad e integridad.	Sí	El Central de Riesgo deberá seguir lo detallado en los manuales de los equipos para poder cumplir con el mantenimiento de los mismos y esporádicamente contratar servicios de mantenimiento siempre y cuando sea necesario.
			Ubicación en un área susceptible de inundación	Inundación										
A19	Generar Venta por Web / Generar Venta de Servicios Complementarios / Generar Servicios Etapa Prospección	Correo electrónico	Falta de políticas para el uso del correo electrónico	Uso no autorizado del equipo	IDR52	Debido a que el personal de la Central de Riesgo desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internas relacionadas con el uso de correo electrónico pudiendo generar debilidades y vulnerabilidades de seguridad.	5	3	7	13.2.1	Information involved in electronic messaging should be appropriately protected.	Se deberán elaborar guías de clasificación de la información en base a distintos aspectos de manera que se pueda asegurar la pretección de la misma.	Sí	Actualmente el Central de Riesgo cuenta con algunas tipificaciones de información. Debe establecer una clasificación para la inormación de manera que sea valida para toda la organización y de esta forma poder respetar la clasificación en cada instalción que esta sea procesada.
			Entrenamiento insuficiente en seguridad	Error en el uso										
			Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Abuso de los derechos	IDR53	Debido a un inadecuado procedimiento de contratación como la evidencia de antecedentes penales y policiales, desarrollo de pruebas de competencia, desconocimiento de las normas, políticas y criterios de seguridad de información y falta de disposiciones en contratos se incumplan las normas internas pudiendo generar debilidades y vulnerabilidades en la seguridad de la Central de Riesgo.	5	4	8					

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A19	Generar Venta por Web / Generar Venta de Servicios Complementarios / Generar Servicios Etapa Prospección	Correo electrónico	Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Falsificación y Abuso de derechos	IDR54	Debido a la falta de procesos disciplinarios en caso de incidentes de seguridad a través del uso del correo electrónico no sea posible tomar acciones correctivas.	5	3	7	16.1.1	Information involved in electronic messaging should be appropriately protected.	Se deberán elaborar guías de clasificación de la información en base a distintos aspectos de manera que se pueda asegurar la pretección de la misma.	Sí	Actualmente el Central de Riesgo cuenta con algunas tipificaciones de información. Debe establecer una clasificación para la inormación de manera que sea valida para toda la organización y de esta forma poder respetar la clasificación en cada instalción que esta sea procesada.
A20	Generar Venta por Web / Generar Venta de Servicios Complementarios	Servidor de Correo	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información	IDR55	Debido a la falta de mantenimiento, el envío de correos electrónicos se vea interrumpido	5	3	7	11.2.4	Instalación y protección de equipos: f) se deberían vigilar las condiciones ambientales, como temperatura y humedad, que puedan afectar negativamente al funcionamiento de los equipos de tratamiento de información	La Central de Riesgo deberá vigilar las condiciones ambientales, como temperatura y humedad, que puedan afectar negativamente al funcionamiento de los equipos en los cuales se da tratamiento o es almacenada la información.	Sí	Se deberá averiguar sobre las condiciones físicas pertinentes al lugar en el cual está la sede dLa Central de Riesgo. Determinar y acondicionar un área en la cual se pueda asegurar la integridad física de los equipos de tratamiento de información.
			Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento										
			Almacenamiento sin protección	Hurto de información	IDR56	Debido a inadecuados procedimientos de custodia y falta de procedimientos para copias, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio, pudiendo afectar la disponibilidad e integridad de la información.	5	3	7					
			Copia no controlada	Hurto de información										
			Falta de protección física de las puertas y ventanas de la edificación	Hurto de Servidor										

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A51	Generar Venta por Web / Generar Venta de Servicios Complementarios	Personal de Tecnología de Información	Ausencia del personal	Incumplimiento en la disponibilidad del personal	IDR74	Debido a que el personal desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	5	4	8	7.2.4	El accesos al código fuente debe ser restringido	Se deberán elaborar guías de clasificación de la información en base a distintos aspectos de manera que se pueda asegurar la pretección de la misma.	Sí	Actualmente el Central de Riesgo cuenta con algunas tipificaciones de información. Debe establecer una clasificación para la inormación de manera que sea valida para toda la organización y de esta forma poder respetar la clasificación en cada instalción que esta sea procesada.
			Procedimientos inadecuados de contratación	Destrucción de equipos o medios										
			Entrenamiento insuficiente en seguridad	Error en el uso										
			Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos	IDR75	Debido a que no se encuentre actualizada la relación de aplicativos (cliente/servidor y host) vs. owners, se otorguen o eliminen accesos a empleados de TI sin contar con todas las aprobaciones requeridas, pudiendo facilitar la divulgación de información.	5	4	8	7.1.2	Toda la información y los activos asociados con las instalaciones de procesamiento de información deben ser propiedad de una de una parte determinada de la organización.	La Central de Riesgo deberá otorgar accesos a el personal que lo necesite, restringiendo las funciones de sistema que no sean necesarias para cada empleado.	Sí	La Central de Riesgo deberá establecer las restricción en base a perfiles que se les dará a sus empleados de manera que tengan sólo acceso a las funciones necesarias para ellos. Esto se logrará a medida que se logre implantar en cada sistema.

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A51	Generar Venta por Web / Generar Venta de Servicios Complementarios	Personal de Tecnología de Información	Trabajo no supervisado	Hurto de información o medios	IDR76	Debido a la falta de supervisión del personal de TI, personas a las que no corresponde cuenten con accesos a los que ya no están autorizados, pudiendo generarse fuga y/o robo de información.	5	4	8	7.1.2	Toda la información y los activos asociados con las instalaciones de procesamiento de información deben ser propiedad de una de una parte determinada de la organización.	La Central de Riesgo deberá otorgar accesos a el personal que lo necesite, restringiendo las funciones de sistema que no sean necesarias para cada empleado.	Sí	La Central de Riesgo deberá establecer las restricción en base a perfiles que se les dará a sus empleados de manera que tengan sólo acceso a las funciones necesarias para ellos. Esto se logrará a medida que se logre implantar en cada sistema.
			Falta de protección física de las puertas	Hurto de equipo	IDR77	Debido a insuficientes políticas de protección, los equipos se encuentren desprotegidos y atacantes externos aprovechen vulnerabilidades.	5	4	8					
			Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR78	Por incumplimiento de procedimientos, se produzcan ataques informáticos a aplicaciones del negocio, pudiendo provocar indisponibilidad y/o falta de integridad de las aplicaciones.	5	4	8	6.2.3	Acuerdos con terceros relacionados con el acceso, tratamiento, comunicación o gestión de la información de la organización o las instalaciones de procesamiento de información, o la adición de productos o servicios a instalaciones de procesamiento de información debe cubrir todos los requisitos de seguridad pertinentes.			
			Falta de proceso formal para la revisión (supervisión) de los derechos de acceso											
			Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con terceros											

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A51	Generar Venta por Web / Generar Venta de Servicios Complementarios	Personal de Tecnología de Información	Falta o insuficiencia en el acuerdo a nivel de servicio (terceros)	Incumplimiento en el mantenimiento del sistema de información	IDR79	Por falta de disposiciones en contratos, personal deshonesto que tenga acceso a equipos o aplicativos que poseen información crítica para el negocio del Banco, pudiendo afectar la integridad y/o disponibilidad de la información.	5	4	8	9.4.5	La verificación de antecedentes en todos los candidatos debe llevarse a cabo de acuerdo con las leyes, regulaciones y ética, y proporcional a los requerimientos del negocio, a la clasificación de la información que se accede, y a los riesgos percibidos.	La Central de Riesgo deberá otorgar accesos a el personal que lo necesite, restringiendo las funciones de sistema que no sean necesarias para cada empleado.	Sí	La Central de Riesgo deberá establecer las restricción en base a perfiles que se les dará a sus empleados de manera que tengan sólo acceso a las funciones necesarias para ellos. Esto se logrará a medida que se logre implantar en cada sistema.
A22	Generar Venta de Servicios Complementarios	Equipo Telefónico	Líneas de comunicación sin protección Tráfico sensible sin protección	Escucha subrepticia	IDR198	Divulgación de la información relacionada con el servicio brindado y como consecuencia pérdida de la confidencialidad	5	2	6	5.1.2	Políticas y procedimientos para el intercambio de información y software: Se deberían establecer políticas, procedimientos y controles formales de intercambio con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación. a) los procedimientos designados para proteger la información intercambiada de una intercepción	La Central de Riesgo debe establecer un procedimiento formal de intercambio de información que con el fin de proteger la información durante el intercambio de la misma.	Sí	La central debería tener identificada la información en todo momento y saber donde se encuentra y quien accede a esta. Para este caso se encontró que las fchas con el nivel del alumno están expuestas a modificaciones y por ende podrían ser ingresadas como data corrupta al sistema. Por estos motivos se debe establecer el procedimiento de intercambio de información durante este proceso de manera que se evite estás exposiciones inseguras.

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A23	Generar Venta de Servicios Complementarios	Personal Comercial - Ventas	Procedimientos inadecuados de contratación	Error en el uso de aplicativos Destrucción de equipos Procesamiento ilegal de los datos	IDR200	Por incumplimiento de procedimientos, se produzcan ataques informáticos a aplicaciones del negocio, o a equipos como servidores pudiendo provocar indisponibilidad y/o falta de integridad de las aplicaciones e información de Titulares	5	4	8	7.2.2	Los roles y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceras partes deben ser definidas y documentadas, de conformidad con la política de información de la organización de seguridad.	Las sesiones a los sistemas y conexiones de red del Central de Riesgo deberán ser finalizadas luego de un periodo definido d e inactividad.	Sí	Al igual que las sesiones de sistema, las sesiones activas a las distintas aplicaciones del Central de Riesgo deberán ser finalizadas luego de un periodo definido de tiempo. Esto se puede lograr estableciendo dichas condiciones en los aplicativos que son mantenidos por el Central de Riesgo, de manera que pueda establecerse la finalización de la sesión en cada aplicativo.
			Falta de procedimiento formal para el registro y retiro del registro de usuario Falta de proceso formal para la revisión (supervisión) de los derechos de acceso Falta de procedimiento de monitoreo de los recursos de procesamiento información	Abuso de los derechos	IDR201	Debido a inadecuado procedimiento de baja de accesos, personal no pueda realizar sus labores por la falta de accesos a los diferentes sistemas, generando improductividad.	5	4	8					
			Falta de políticas sobre el uso del correo electrónico	Error en el uso	IDR202	Por falta de políticas para el uso del correo electrónico, se generen debilidades y vulnerabilidades de seguridad (ataques informáticos) y se divulgue información o se pierda la integridad de la misma	5	3	7	9.1.2	Eventos seguridad de la información debe ser reportada a través de canales de gestión adecuadas tan pronto como sea posible.	El Central de Riesgo debe identificar, documentar e implementar las reglas para un uso aceptable del correo electrónico.	Sí	Como parte de la educación organizacional que se brinda (de alguna forma) a los trabajadores, la Central de Riesgo deberá indicar las normas claras para el uso del correo electrónico que se les otorga.
			Falta de procedimientos para la introducción del software en los sistemas operativos		IDR203	Debido a la falta de procedimientos para la introducción de sw y una actitud deshonesta del personal de ventas, exista fraude interno, generandose fuga y/o robo de información.	5	3	7					

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A24	Generar Venta de Servicios Complementarios	CD encriptado	Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del CD Polvo, corrosión	IDR209	Por inadecuadas políticas de almacenamiento, se dañen CDs que almacenan información crítica para el negocio de la Central, pudiendo afectar la integridad y/o disponibilidad de la información.	5	2	6	8.3.1	Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollado e implementado.	El Central de Riesgo debería mantener una política de uso de medidas criptográficas para porteger la información transportada en las líneas de comunicación.	No	La Central de Riesgo no cuenta con especialistas dedicados unicamentes a las redes. Lo que se ha logrado hasta el momento para establecer lo necesario en red es realizado por personas encargadas del area de tecnología e información. Actualmente no es aplicable este control ya que demanda la contratación de personas especialistas en redes y creación de puestos para los mismos.
			Almacenamiento sin protección	Hurto o destrucción de CD	IDR210	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a los Cds que almacenan información crítica para el negocio de la Central de Riesgo, pudiendo afectar la integridad y/o disponibilidad de la información o Robo	5	3	7					
			Copia no controlada											
			Trabajo no supervisado del personal externo o de limpieza											

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A26	Generar Venta de Servicios Complementarios	Operadores	Ausencia del personal	Incumplimiento en la disponibilidad del personal	IDR211	Debido a la falta de disponibilidad de operadores, haya un grave impacto en la productividad del negocio	5	4	8	6..1.1	Una política de control de acceso debe ser establecido, documentado y revisado sobre la base de los negocios y los requisitos de seguridad para el acceso.	El Central de Riesgo deberá otorgar accesos a el personal que lo necesite, restringiendo las funciones de sistema que no sean necesarias para cada empleado.	Sí	El Central de Riesgo deberá establecer las restricción en base a perfiles que se les dará a sus empleados de manera que tengan sólo acceso a las funciones necesarias para ellos. Esto se logrará a medida que se logre implantar en cada sistema.
			Procedimientos inadecuados de contratación	Destrucción de equipos o medios	IDR212	Debido a que el personal desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	5	5	9	7.2.2	Toda la información y los activos asociados con las instalaciones de procesamiento de información deben ser propiedad de una parte designada de la organización.	El Central de Riesgo deberá otorgar accesos a el personal que lo necesite, restringiendo las funciones de sistema que no sean necesarias para cada empleado.	Sí	El Central de Riesgo deberá establecer las restricción en base a perfiles que se les dará a sus empleados de manera que tengan sólo acceso a las funciones necesarias para ellos. Esto se logrará a medida que se logre implantar en cada sistema.
			Entrenamiento insuficiente en seguridad	Error en el uso de aplicaciones										
			Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos	IDR213	Debido a que no se cuente con una relación de aplicativos (cliente/servidor y host) vs. owners, se otorguen o eliminen accesos a operadores sin contar con todas las aprobaciones requeridas, pudiendo facilitar la divulgación de información y/o pérdida de integridad de la información	5	4	8	9.1.1	La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares a través de un proceso formal.	Las sesiones a los sistemas y conexiones de red del Central de Riesgo deberán ser finalizadas luego de un periodo definido d e inactividad.	Sí	Al igual que las sesiones de sistema, las sesiones activas a las distintas aplicaciones del Central de Riesgo deberán ser finalizadas luego de un periodo definido de tiempo. Esto se puede lograr estableciendo dichas condiciones en los aplicativos que son mantenidos por el Central de Riesgo, de manera que pueda establecerse la finalización de la sesión en cada aplicativo.
			Trabajo no supervisado del personal	Hurto de medios o documentos	IDR214	Debido a la falta de supervisión del personal, personas a las que no corresponde cuenten con accesos a los que ya no están autorizados, pudiendo generarse fuga y/o robo de información.	5	4	8	8.1.1	Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes a las instalaciones de procesamiento de información y la información deben ser retirados a la terminación de su empleo, contrato o acuerdo, o ajustarse a los cambios.			

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A26	Generar Venta de Servicios Complementarios	Operadores	Falta de reportes sobre fallas incluidos en los registros de operadores	Abuso de los derechos	IDR215	Debido a falta de procedimientos de registros de bitácora, no se puedan tomar acciones correctivas por tanto no se registren acciones correctivas alrededor de los incidentes en las actividades diarias	4	3	6	16.1.,1	Registro de la auditoria: Los registros de auditoria grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados para un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso.	La Central de Riesgo debe establecer un mecanismo (cámaras de vigilancia) con el cual sea capaz de mantener un registro de las acciones realizadas por sus empleadores y/o personas que se encuentran en las instalaciones de la organización con el fin de asegurar un monitereo a sobre los activos de información de la organización.	Sí	La organización cuenta actualmente con un sector de las instalaciones monitoreado por un pequeño circuito de cámaras de vigilancia. Debería expandir este mecanismo al resto de sectores para de esta manera poder monitorear las actividades que realizan sus empleados y también porder seguir de cerca las incidencias que podrían darse con los activos de información en este caso con los documentos de traducción que se alamacenan y los exámenes de clasificación.
			Falta de registros en las bitácoras *(logs)	Error en el uso	IDR215	Debido a falta de procedimientos de registros de bitácora, no se puedan tomar acciones correctivas por tanto no se registren acciones correctivas alrededor de los incidentes en las actividades diarias	4	3	6	16.1.3	Registro de la auditoria: Los registros de auditoria grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados para un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso.	La Central de Riesgo debe establecer un mecanismo (cámaras de vigilancia) con el cual sea capaz de mantener un registro de las acciones realizadas por sus empleadores y/o personas que se encuentran en las instalaciones de la organización con el fin de asegurar un monitereo a sobre los activos de información de la organización.	Sí	La organización cuenta actualmente con un sector de las instalaciones monitoreado por un pequeño circuito de cámaras de vigilancia. Debería expandir este mecanismo al resto de sectores para de esta manera poder monitorear las actividades que realizan sus empleados y también porder seguir de cerca las incidencias que podrían darse con los activos de información en este caso con los documentos de traducción que se alamacenan y los exámenes de clasificación.
			Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos	IDR216	Debido a la falta de disposiciones en los contratos y a una actitud deshonesta del personal, exista fraude interno, generandose fuga y/o robo de información o pérdida de su integridad	5	5	9					

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A27	Generar Venta de Servicios Complementarios	Documento Excel con el registro de los Servicios (Macro)	Trabajo no supervisado del personal externo o de limpieza	Hurto de documento	IDR217	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a información confidencial, divulgándola a la competencia por ejemplo.	5	4	8	8.2.1	Restricción de acceso a la información: Se debería dar acceso a la información y a las funciones del sistema de aplicaciones sólo a los usuarios de éste, incluido el personal de apoyo, de acuerdo con una política de control de accesos definida.	La Central de Riesgo deberá otorgar accesos a el personal que lo necesite, restringiendo las funciones de sistema que no sean necesarias para cada empleado.	Sí	La Central de Riesgo deberá establecer las restricción en base a perfiles que se les dará a sus empleados de manera que tengan sólo acceso a las funciones necesarias para ellos. Esto se logrará a medida que se logre implantar en cada sistema.
			Falta o insuficiencia de políticas sobre limpieza de escritorio y de pantalla	Uso no autorizado del equipo	IDR218	Debido a la falta de políticas internas, personal no autorizado acceda a iinformación crítica (personal de limpieza)	5	4	8					
			Falta de control eficaz del cambio y protección de documento	Mal funcionamiento / acceso no autorizado	IDR219	Personal de actitud deshonesta acceda al documento, o personal no autorizado logre acceder por un mal funcionamiento, generándose pérdida de la intgegridad o robo de información	5	4	8					
A29	Generar Venta de Servicios Complementarios	Servidores de Archivos	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información	IDR223	Debido a la falta de mantenimiento, el acceso a la Base de Datos se vea interrumpido	5	2	6	11.2.6	Instalación y protección de equipos: f) se deberían vigilar las condiciones ambientales, como temperatura y humedad, que puedan afectar negativamente al funcionamiento de los equipos de tratamiento de información	La Central de Riesgo deberá vigilar las condiciones ambientales, como temperatura y humedad, que puedan afectar negativamente al funcionamiento de los equipos en los cuales se da tratamiento o es almacenada la información.	Sí	Se deberá averiguar sobre las condiciones físicas pertinentes al lugar en el cual está la sede dLa Central de Riesgo. Determinar y acondicionar un área en la cual se pueda asegurar la integridad física de los equipos de tratamiento de información.
			Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento										
			Almacenamiento sin protección	Hurto de información	IDR224	Por inadecuadas políticas de acceso personal no autorizado tenga acceso a servidores de archivos que contienen nformación crítica para el negocio, pudiendo afectar la integridad y/o disponibilidad de la información.	4	3	6					
			Copia no controlada	Hurto de información										
			Falta de protección física de las puertas y ventanas de la edificación	Hurto de Servidor	IDR225	Debido a inadecuados procedimientos de custodia, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio de la Central, pudiendo afectar la disponibilidad e integridad de la información.	5	3	7					
			Falta de autorización de los recursos de procesamiento de la información											

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A30	Generar Venta de Servicios Complementarios	Intranet de la Central de Riesgo	Interfaz de usuario complicada	Error en el uso	IDR226	Debido a una interfaz complicada se realice una errónea asignación de perfiles definidos para los roles del personal.	4	2	5	13.2.4	Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal, y una técnica de autenticación adecuado debe ser elegido para demostrar la identidad alegada de un usuario.	El Central de Riesgo deberá definir un conjunto adecuado de procedimientos para marcar y tratar la información de acuerdo con el esquema de clasificación adoptado previamente.	Sí	Actualmente el Central de Riesgo cuenta con algunas tipificaciones de información. Debe establecer una clasificación para la inormación de manera que sea valida para toda la organización y de esta forma poder respetar la clasificación en cada instalción que esta sea procesada.
			Falta de documentación y actualización de dicha documentación		IDR227	Por falta de documentación (manuales, procedimientos, reporte de turnos e indicadores de gestión), haya la posibilidad de fallas en el otorgamiento de accesos generando fuga de información	4	4	7					
			Falta de mecanismos de identificación y autentificación	Falsificación de derechos	IDR228	Por incumplimiento de norma de identificación de usuarios y/o procedimiento de elaboración de reporte, no sea posible identificar a usuario que realizó uso inadecuado de accesos y se dificulten las acciones correctivas.	5	4	8					
			Gestión deficiente de las contraseñas		IDR229	Debido a inadecuada poítica de otorgamiento de accesos, los accesos de los usuarios que se encuentren de vacaciones no sean deshabilitados durante ese período, pudiendo ser vulnerados por un tercero.	4	4	7					
			Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos										

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A31	Generar Venta de Servicios Complementarios	Medios de Almacenamiento	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información	IDR230	Debido a la falta de mantenimiento, el acceso a la Base de Datos se vea interrumpido	5	2	6	8.3.2	La protección física contra daños por incendio, inundación, terremoto, explosión, disturbios civiles y otras formas de desastres naturales o de origen humano deben ser diseñados y aplicados.	La Central de Riesgo deberá minimalizar las indicaciones del propósito de sus oficinas, sin signos obvios, fuera o dentro del edificio, que identifiquen la presencia de actividades de tratamiento de información en ellas.	Sí	Se deberá evaluar todas la simbología establecida en las instalaciones y distintas sedes del Central de Riesgo a medida que se determine el propósito de cada símbolo y se pueda retirar lo que sea inadecuado.
			Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento										
			Almacenamiento sin protección	Hurto de medios	IDR231	Por inadecuadas políticas de acceso personal no autorizado tenga acceso a servidores de archivos que contienen nformación crítica para el negocio, pudiendo afectar la integridad y/o disponibilidad de la información.	5	3	7	8.3.3	Debe haber procedimientos establecidos para la gestión de medios extraíbles.	El Central de Riesgo deberá definir un conjunto adecuado de procedimientos para marcar y tratar la información de acuerdo con el esquema de clasificación adoptado previamente.	Sí	Actualmente la Central de Riesgo cuenta con tipificaciones de información. Debe establecer una clasificación para la inormación de manera que sea valida para toda la organización y de esta forma poder respetar la clasificación en cada instalción que esta sea procesada.
			Copia no controlada											

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A31	Generar Venta de Servicios Complementarios	Medios de Almacenamiento	Falta de conciencia acerca de la seguridad	Error en el uso	IDR232	Debido a que el personal desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	5	3	7	8.3.1	Debe haber procedimientos establecidos para la gestión de medios extraíbles.	El Central de Riesgo deberá definir un conjunto adecuado de procedimientos para marcar y tratar la información de acuerdo con el esquema de clasificación adoptado previamente.	Sí	Actualmente el Central de Riesgo cuenta con algunas tipificaciones de información. Debe establecer una clasificación para la inormación de manera que sea valida para toda la organización y de esta forma poder respetar la clasificación en cada instalción que esta sea procesada.
			Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios	IDR233	Debido a una inadecuada gestión de los accesos , personal no autorizado pueda acceder al centro de operaciones, pudiendo provocar daños a equipos y robo de medios de almacenamiento	4	4	7					
			Falta de protección física de las puertas y ventanas de la edificación	Hurto de Medios de Almacenamiento										
			Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con terceras partes	Abuso de los derechos	IDR234	Debido a la falta de disposiciones en los contratos y a una actitud deshonesta del personal, exista fraude interno, generandose robo de información.	5	4	8					
			Falta de autorización de los recursos	Hurto de medios	IDR235	Por inadecuadas políticas de acceso (por ejem: fallas en custodia de los medios de almacenamiento) personal no autorizado tenga acceso a medios que almacenan información crítica para el negocio de la Central, pudiendo afectar la integridad y/o disponibilidad de la información.	5	3	7					

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A33	Generar Venta de Servicios Complementarios	Microsoft Office	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Mal funcionamiento de sw	IDR236	Debido al mal funcionamiento del sw, no se puedan realizar las actividades diarias (p.e. elaboraciones de reportes) generando improductividad en el negocio.	5	2	6	9.4.1	Procedimientos adecuados deben ser implementados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso de materiales respecto de los cuales puede haber derechos de propiedad intelectual y sobre el uso de productos de software propietario.	La Central de Riesgo debe establecer un procedimiento formal de intercambio de información que con el fin de proteger la información durante el intercambio de la misma.	Sí	El centro debería tener identificada la información en todo momento y saber donde se encuentra y quien accede a esta. Para este caso se encontró que las fchas con el nivel del alumno están expuestas a modificaciones y por ende podrían ser ingresadas como data corrupta al sistema. Por estos motivos se debe establecer el procedimiento de intercambio de información durante este proceso de manera que se evite estás exposiciones inseguras.
A34	Generar Venta de Servicios Complementarios	Infraestrucutra de red	Falta de prueba del envío o la recepción de mensajes	Negación de acciones	IDR237	Debido a la falta de pruebas, personal no pueda realizar el envío de mensajes imposibilitando sus labores cotidianas y la entrega de servicios afectando la operabilidad y productividad del negocio	5	2	6	13.1.1	Las características de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en un contrato de servicios de red, si estos servicios se proporcionan *inhouse* o subcontratado.	El Central de Riesgo debe definir un procedimiento claro para el manejo de sus activos de información durante sus procesos y de esta forma asegurar que esten protegidos y evitar el aceso de peronas no autorizadas a estos.	Sí	El Central de Riesgo deberá analizar los procesos afectados y de esta manera corregir las deficiencias encontradas (ausencia de personal) que podrían acpntecer con incidencias de seguridad.
			Tráfico sensible sin protección	Saturación del sistema de información	IDR238	Debido al tráfico y a inadecuados procesos de detección, los intentos no autorizados de acceso a información de aplicativos no sean detectados y se produzcan ataques informáticos.	5	3	7	13.1.2	Los usuarios sólo deben estar provistos de acceso a los servicios que han sido específicamente autorizado a usar.	El Central de Riesgo debe establecer un procedimiento formal de intercambio de información que con el fin de proteger la información durante el intercambio de la misma.	Sí	El centro debería tener identificada la información en todo momento y saber donde se encuentra y quien accede a esta. Para este caso se encontró que las fchas con el nivel del alumno están expuestas a modificaciones y por ende podrían ser ingresadas como data corrupta al sistema. Por estos motivos se debe establecer el procedimiento de intercambio de información durante este proceso de manera que se evite estás exposiciones inseguras.
			Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones	IDR239	Debido a la falta de mantenimieniento de la infraestructura, la red no se encuentre disponible imposbilitando la entrega del servicio.	5	2	6	13.1.3	Identificación de equipo automático debe ser considerada como un medio para autenticar las conexiones de ubicaciones específicas y equipo.	La Central de Riesgo deberá otorgar accesos al personal que lo necesite, restringiendo las funciones de sistema que no sean necesarias para cada empleado.	Sí	La Central de Riesgo deberá establecer la restricción en base a perfiles que se les dará a sus empleados de manera que tengan sólo acceso a las funciones necesarias para ellos. Esto se logrará a medida que se logre implantar en cada sistema.

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A34	Generar Venta de Servicios Complementarios	Infraestrucutra de red	Arquitectura insegura de la red	Espionaje remoto	IDR240	Debido a una arquitectura insegura se produzcan ataques informáticos a las principales aplicaciones del negocio , pudiendo incluso provocar indisponibilidad y/o falta de integridad de las aplicaciones.	5	3	7	13.1.2	Las redes deben ser adecuadamente gestionados y controlados, con el fin de ser protegidos de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Las sesiones a los sistemas y conexiones de red del Central de Riesgo deberán ser finalizadas luego de un periodo definido d e inactividad.	Sí	Al igual que las sesiones de sistema, las sesiones activas a las distintas aplicaciones del Central de Riesgo deberán ser finalizadas luego de un periodo definido de tiempo. Esto se puede lograr estableciendo dichas condiciones en los aplicativos que son mantenidos por el Central de Riesgo, de manera que pueda establecerse la finalización de la sesión en cada aplicativo.
			Conexiones de red pública sin protección	Uso no autorizado del equipo	IDR241	Debido a insuficientes políticas de protección, los equipos se encuentren desprotegidos y atacantes externos aprovechen vulnerabilidades.	5	3	7					
A35	Generar Venta de Servicios Complementarios	Dominio Organizativo	Falta de identificación y autentificación de emisor y receptor	Falsificación de derechos	IDR242	Debido a una falta de políticas de seguridad para la identificación y autenticación de emisor y receptor e inadecuados procesos de detección, los intentos no autorizados de acceso a información de aplicativos no sean detectados y se produzcan ataques informáticos.	5	3	7					
			Transferencia de contraseñas autorizadas	Espionaje remoto	IDR243	Divulgación de la información relacionada con el servicio brindado y como consecuencia pérdida de la confidencialidad	5	4	8					
A36	Generar Venta de Servicios Complementarios	Edificio	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios	IDR244	Debido a inadecuadas políticas de seguridad para el acceso físico al edificio, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio del Banco, pudiendo afectar la integridad y/o disponibilidad de la información.	5	3	7	11.1.2	Las áreas seguras deberían estar protegidos por controles de entrada adecuados para garantizar que sólo el personal autorizado tiene acceso permitido.	El Central de Riesgo deberá otorgar accesos a el personal que lo necesite, restringiendo las funciones de sistema que no sean necesarias para cada empleado.	Sí	El Central de Riesgo deberá establecer las restricción en base a perfiles que se les dará a sus empleados de manera que tengan sólo acceso a las funciones necesarias para ellos. Esto se logrará a medida que se logre implantar en cada sistema.
			Falta de protección física de las puertas y ventanas de la edificación	Hurto de equipo										
			Red energética inestable	Pérdida del suministro de energía	IDR245	Debido a una falta de mantenimiento de las instalaciones se genera una pérdida del suministro de energía generando indisponibilidad de los servicios.	5	3	7					

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A52	Generar Venta de Servicios Complementarios	Personal de Atención al cliente	Entrenamiento insuficiente en seguridad	Hurto de información	IDR255	Debido a que el personal de la Central desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	5	4	8	7.1.2	La protección de datos y privacidad debe garantizarse a lo dispuesto en la legislación pertinente, los reglamentos, y, si procede, las cláusulas contractuales.	El Central de Riesgo deberá validar los datos de entrada a las aplicaciones del sistema para garantizar su correctitud. Deberá hacerse una revisión periódica de los mismo.	Sí	El Central de Riesgo debera revisar periódicamente los parámetros necesarios para el funcionamiento de sus aplicaciones de manera que estas adopten la realidad a la cual está circunscrita la organización. Estos parámetros serán mantenidos por un encargado y es el quién deberá velar por la correctitud de los mismos.
			Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo										
			Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR256	Debido a que no se cuenta con una relación de aplicativos (cliente/servidor y host) vs. owners, se otorguen o eliminen accesos sin contar con todas las aprobaciones requeridas, pudiendo facilitar la divulgación de información y el hurto de Información, ocasionando grandes pérdidas financieras	4	3	6	7.2.2	Los requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados y revisados regularmente.	El Central de Riesgo debe identificar, documentar e implementar las reglas para un uso aceptable del correo electrónico.	Sí	Como parte de la educación organizacional que se brinda (de alguna forma) a los trabajadores, el Central de Riesgo deberá indicar las normas claras para el uso del correo electrónico que se les otorga.
			Falta de proceso formal para la revisión (supervisión) de los derechos de acceso											

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A52	Generar Venta de Servicios Complementarios	Personal de Desarrollo	Falta de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones	IDR256	Debido a que no se cuenta con una relación de aplicativos (cliente/servidor y host) vs. owners, se otorguen o eliminen accesos sin contar con todas las aprobaciones requeridas, pudiendo facilitar la divulgación de información y el hurto de Información, ocasionando grandes pérdidas financieras	4	3	6	12.1.4 12.1.2	Los requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados y revisados regularmente.	El Central de Riesgo debe identificar, documentar e implementar las reglas para un uso aceptable del correo electrónico.	Sí	Como parte de la educación organizacional que se brinda (de alguna forma) a los trabajadores, el Central de Riesgo deberá indicar las normas claras para el uso del correo electrónico que se les otorga.
			Falta de políticas sobre el uso del correo electrónico	Error en el uso										
			Falta de procedimientos para la introducción del software en los sistemas operativos											
			Falta de procedimientos para el manejo de información clasificada											
			Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos										
			Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo o información										
A78	Generar Venta de Servicios Complementarios	Personal Servicio al Cliente	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo	IDR257	Debido a actitud deshonesta del personal, exista fraude interno al no realizar las bajas o cambios de roles oportunamente, generandose fuga y/o robo de información.	5	4	8	12.1.1	La verificación de antecedentes en todos los candidatos debe llevarse a cabo de acuerdo con las leyes, regulaciones y ética, y proporcional a los requerimientos del negocio, a la clasificación de la información que se accede, y a los riesgos percibidos.	Se deberán elaborar guías de clasificación de la información en base a distintos aspectos de manera que se pueda asegurar la pretección de la misma.	Sí	Actualmente la Central de Riesgo cuenta con algunas tipificaciones de información. Debe establecer una clasificación para la inormación de manera que sea valida para toda la organización y de esta forma poder respetar la clasificación en cada instalción que esta sea procesada.
			Falta de revisiones de los derechos de acceso	Abuso de los derechos										

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A41	Generar Venta de Servicios Complementarios	Aplicación Web de Seguimiento	Distribución errada de los derechos de acceso	Abuso de los derechos	IDR258	Acceso no autorizado pudiendo generar indisponibilidad del acceso al aplicativo	5	3	7	12.7.1	Gestión de contraseñas de usuario: Se debería controlar la asignación de contraseñas por medio de un proceso de gestión formal. a) requerir que los usuarios firmen un compromiso para mantener en secreto sus contraseñas personales y las compartidas por un grupo sólo entre los miembros de ese grupo.	La Central de Riesgo debe controlar la asignación de contraseñas mediante un proceso formal en el cual designe la responsabilidad sobre estas a los dueños de las mismas.	Sí	La Central de Riesgo deberá mejorar la forma en la que asigna ya la asignación de contraseñas y no dejar relegada esta gestión ya que depende de ella se otorgan accesos a la información. Para el caso, será necesario establecer registros en los cuales se cuente con la identificación de usuarios y sus respectivas contraseñas.
			Falta de documentación y actualización de dicha documentación	Error en el uso	IDR259	Por falta de documentación (manuales, procedimientos, reporte de turnos e indicadores de gestión), haya la posibilidad de fallas en el otorgamiento de accesos generando fuga de información	4	4	7				
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos	IDR260	Debido a la falta de autentificación personal no autorizado acceda al aplicativo y se produzcan ataques a la aplicación	5	3	7				
A63	Generar Venta de Servicios Complementarios	Sistema de decisiones	Interfase de usuario complicada	Error en el uso	IDR261	Debido a la falta de documentacion , halla una una falla en la designación de perfiles y roles y configuración de parámetros pudiendo generar fallas en la entrega del servicio, improductividad y accesos no autorizados.	4	4	7	9.4.3	Restricción de acceso a la información: Se debería dar acceso a la información y a las funciones del sistema de aplicaciones sólo a los usuarios de éste, incluido el personal de apoyo, de acuerdo con una política de control de accesos definida.	La Central de Riesgo deberá otorgar accesos a el personal que lo necesite, restringiendo las funciones de sistema que no sean necesarias para cada empleado.	Sí	La Central de Riesgo deberá establecer la restricción en base a perfiles que se les dará a sus empleados de manera que tengan sólo acceso a las funciones necesarias para ellos. Esto se logrará a medida que se logre implantar en cada sistema.
			Falta de documentación											
			Configuración incorrecta de parámetros											
			Falta de control eficaz del cambio	Mal funcionamiento del software	IDR262	Fallas en el funcionamiento de los aplicativos generando vulnerabildiades en la seguridad, accesos no autorizados, robo de información.	5	3	7				

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A48	Generar Venta de Servicios Complementarios	Web Service	Especificaciones incompletas o no claras para los desarrolladores Software nuevo o inmaduro	Mal funcionamiento	IDR265	Debido al mal funcionamiento del sw, no se puedan realizar las actividades diarias (p.e. envío y recepción de solicitudes por por parte del cliente) generando improductividad en el negocio.	5	4	8	13.2.4 13.2.1	Oportunidades para la filtración de información debe ser evitado.	El Central de Riesgo deberá ejercer un entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales a todos los empleados de la organización y donde sea relevante.	Sí	Se deberá encargar a las direcciones del Central de Riesgo dicho entrenamiento de manera que todos los empleados estén al tanto de las dispocisiones realizadas en la organización.
			Falta o insuficiencia de la prueba del software Defectos bien conocidos en el software	Abuso de los derechos	IDR266	Acceso no autorizado pudiendo generar indisponibilidad del acceso a los aplicativos, pérdida de la integridad de la infrmación	5	4	8					
			Configuración incorrecta de parámetros Falta de documentación Habilitación de servicios innecesarios	Error en el uso Procesamiento ilegal de datos	IDR267	Pérdida en la itnegridad de la información	5	4	8					
A83	Generar Venta de Servicios Complementarios	Laptop	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento	IDR271	Debido a faltas de procedimientos y políticas de almacenamiento, genere un mal funciomamiento en el equipo e indisponibilidad de este para ejecutar las actividades cotidianas, impactandose la productividad de la empresa	5	4	8	8.1.3	Un proceso de autorización de la administración para las nuevas instalaciones de procesamiento de información deben ser definidas e implementadas.	El Central de Riesgo debe identificar, documentar e implementar las reglas para un uso aceptable del correo electrónico.	Sí	Como parte de la educación organizacional que se brinda (de alguna forma) a los trabajadores, el Central de Riesgo deberá indicar las normas claras para el uso del correo electrónico que se les otorga.
			Almacenamiento sin protección Falta de control de los activos que se encuentran fuera de las instalaciones Falta de política formal sobre la utilización de computadores portátiles	Hurto de equipo	IDR272	Debido a inadecuados procedimientos de custodia, personal no autorizado tenga acceso a equipos , pudiendo afectar la disponibilidad e integridad de la información o robo del equipo	5	4	8					

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A84	Generar Venta de Servicios Complementarios	Zonas de acceso reservado	Entrenamiento insuficiente en seguridad al personal	Ingreso de personal no autorizado	IDR273	Debido a una inadecuada gestión de los accesos en la edificación, personal no autorizado pueda acceder, pudiendo provocar daños a equipos y/o robo de información.	5	3	7	11.1.3	La protección física y las directrices para trabajar en las áreas de seguridad deben ser diseñadas y aplicadas.	El Central de Riesgo deberá aplicar protección física sobre determinadas áreas. Las áreas seguras deberían estar cerradas y controlarse periódicamente cuando estén vacías mediante distintos mecanismos (como ya se ha mencionado antes podrían ser cámaras de vigilancia).	Sí	Se deben determinar previamente cuales áreas serán las que necesiten protección. Luego debería aplicarse el monitoreo adecuado a las mismas y la protección física pertinente.
			Trabajo no supervisado del personal externo o de limpieza	Hurto de activos										
			Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de activos										
			Falta de protección física de las puertas y ventanas de la edificación	Hurto de activos										
A72	Generar Venta de Servicios Complementarios	Documento excel con información para el cliente	Falta de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos	IDR274	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a información confidencial	4	3	6	9.1.1	Política de pantalla y escritorio limpio: b) los computadores y terminales deben ser apagados o protegidos con un mecanismo de protección de pantalla o de teclado controlado por contraseña u otro mecanismo de autentificación, cuando estas se encuentren desatendidos y deben ser protegidas por cerraduras clave, contraseñas u otro tipo de control cuando no sean utilizados	Las computadoras dLa Central de Riesgo deberán ser protegidas con un mecanismo de protección de pantalla o de teclado controlado por contraseña u otro mecanismo de autentificación.	Sí	Este control puede implementarse educando al empleado o estableciendo parámetros en el dominio con el que cuenta La Central de Riesgo de manera que se pueda cumplir con la terminación de sesiones activas luego de cierto tiempo.
			Trabajo no supervisado del personal externo o de limpieza	Hurto de infomación	IDR275	Personal de actitud deshonesta acceda al documento, o personal no autorizado logre acceder por un mal funcionamiento, generándose pérdida de la intgegridad o robo de información	4	3	6					
			Falta de mecanismos de identificación y autentificación											

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A85	Generar Venta de Servicios Complementarios	Reportes Excel del Servicio Complementario brindado	Falta de protección física de las puertas	Hurto de documentos	IDR276	Personal de actitud deshonesta acceda al documento, o personal no autorizado logre acceder por falta de políticas de seguridad y monitoreo, generándose pérdida de la intgegridad o robo de información	4	3	6	9.1.1	Procedimientos de manipulación de la información: Los procedimientos para la manipulación y almacenamiento de la información deben ser establecidos para proteger esta información de divulgaciones o usos no autorizados. Restricciones de acceso para identificar al personal no autorizado.	La Central de Riesgo debe definir un procedimiento claro para el manejo de sus activos de información durante sus procesos y de esta forma asegurar que esten protegidos y evitar el aceso de peronas no autorizadas a estos.	Sí	La Central de Riesgo deberá analizar los procesos afectados y de esta manera corregir las deficiencias encontradas (ausencia de personal) que podrían acpntecer con incidencias de seguridad.
			Entrenamiento insuficiente en seguridad	Error en el uso										
			Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos										
			Falta de autorización de los recursos de procesamiento de la información	Hurto de documentos										
			Falta de mecanismos de permisos para el acceso al documento											
A76	Generar Venta de Servicios Complementarios	Documento Cotización	Falta de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos	IDR280	Debido a una inadecuada gestión de accesos, se otorguen mayores accesos a los usuarios de los que se definieron inicialmente o accesos a usuarios no autorizados , posibilitando la pérdida de integridad de la información o robo de información debido al interés de la competencia.	5	3	7	9.1.1	Conocimiento, educación y entrenamiento de la seguridad de información: Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	La Central de Riesgo deberá ejercer un entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales a todos los empleados de la organización y donde sea relevante.	Sí	Se deberá encargar a las direcciones dLa Central de Riesgo dicho entrenamiento de manera que todos los empleados estén al tanto de las dispocisiones realizadas en la organización.
			Trabajo no supervisado del personal externo o de limpieza	Hurto de infomación										
			Falta de mecanismos de permisos para el acceso al documento											
A65	Generar Venta de Servicios Complementarios	Contrato (Clientes)	Falta de revisiones en las disposiciones por parte de la gerencia	Usos no autorizados de hardware y software	IDR281	Debido a una falta de revisión de las disposiciones en los contratos, no se establezcan medidas de seguridad para con los clientes, generando fraudes ,y/o hurto de información o equipos sin la posibilidad de recibir una indemnización por la pérdida financiera generada	5	3	7	18.1.4	Los roles y responsabilidades de seguridad de los empleados y terceras partes deben ser definidos y documentados de acuerdo con la política de información de la organización de seguridad.	La Central de Riesgo deberá ejercer un entrenamiento apropiado a su personal	Sí	Se deberá encargar a las direcciones dLa Central de Riesgo dicho entrenamiento de manera que todos los empleados estén al tanto de las dispocisiones realizadas en la organización.
				Hurto de equipos, documentos o/y información										
				Abuso de los derechos										

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A70	Generar Venta de Servicios Complementarios	Base de Datos	Falta de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos	IDR282	Debido a inadecuados procesos de detección, los intentos no autorizados de acceso a información del Datamart no sean detectados y se produzcan ataques informáticos	5	3	7	18.2.1	El acceso a la información y funcionesdel datamart por los usuarios y personal de apoyo deben limitarse de acuerdo con la política de control de acceso definidas.	El Central de Riesgo deberá otorgar accesos a el personal que lo necesite, restringiendo las funciones de sistema que no sean necesarias para cada empleado.	Sí	El Central de Riesgo deberá establecer las restricción en base a perfiles que se les dará a sus empleados de manera que tengan sólo acceso a las funciones necesarias para ellos. Esto se logrará a medida que se logre implantar en cada sistema.
			Falta de copias de respaldo	Manipulación con software										
A71	Generar Venta de Servicios Complementarios	Host	Falta de planes de continuidad	Falla del equipo	IDR283	Debido a inadecuados procedimientos de custodia, personal no autorizado tenga acceso al Host, el cual procesa toda la información crítica del negocio, impactando gravemente en la disponibilidad, confidencialidad e integridad de la información.	5	2	6	17.2.1	Los eventos que pueden causar interrupciones en los procesos de negocios deben ser identificados, junto con la probabilidad y el impacto de estas interrupciones y sus consecuencias para la seguridad de la información.	El Central de Riesgo deberá otorgar accesos a el personal que lo necesite, restringiendo las funciones de sistema que no sean necesarias para cada empleado.	Sí	El Central de Riesgo deberá establecer las restricción en base a perfiles que se les dará a sus empleados de manera que tengan sólo acceso a las funciones necesarias para ellos. Esto se logrará a medida que se logre implantar en cada sistema.
			Falta de procedimiento de monitoreo	Abuso de los derechos										
			Falta de procedimientos de identificación y evaluación de riesgos											
			Falta de reportes sobre fallas		IDR284	Debido a una inadecuada gestión de los accesos en el centro de cómputo, personal no autorizado pueda acceder, pudiendo provocar daños a equipos y/o robo de información.	5	2	6					

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A30	Generar Venta de Servicios Complementarios	Intranet de la Central de Riesgo	Interfaz de usuario complicada	Error en el uso	IDR285	Debido al incumplimiento del procedimiento, se desbloquee un usuario de forma constante sin validar que este sea victima de un ataque externo o interno, se genere un bloqueo reiterativo de usuario y/o ataque mayor.	5	3	7	13.1.1	Uso de contraseñas: Los usuarios deberían seguir buenas prácticas de seguridad para la selección y uso de sus contraseñas. Mantener la confidencialidad de las contraseñas.	La Central de Riesgo debe difundir las buenas prácticas de seguridad para el trato que se le dan a las contraseñas asignadas.	Sí	La Central de Riesgo deberá establecer y difundir a sus empleadores medidas con las cuales se asegure la confidencialidad de las contraseñas otorgadas.
			Falta de documentación y actualización de dicha documentación											
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos	IDR286	Debido a errores en el procedimiento de baja de usuarios, no se dé de baja o bloquee los accesos a un usuario que cambia de puesto de trabajo, posibilitando el robo y/o fuga de información.	5	3	7					
			Gestión deficiente de las contraseñas											
			Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos										
A54	Generar Venta de Servicios Complementarios	Aplicación para la depuración y enriquecimiento de Data	Gestión deficiente de las contraseñas	Falsificación de derechos	IDR288	Debido a la falta de mecanismos de autenticación e identificación de usuarios / logs insuficientes, no sea posible identificar a usuario y por ende no sea posible tomar acción correctiva.	4	3	6					
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario											
A43	Generar Servicios Etapa Prospección	Aplicación para generar Modelos Estadísticos	Distribución errada de los derechos de acceso	Abuso de los derechos	IDR89	Acceso no autorizado pudiendo generar indisponibilidad del acceso al aplicativo	4	3	6	9.4.1	Validación de los datos de entrada: Se deberían validar los datos de entrada a las aplicaciones del sistema para garantizar que son correctas y apropiadas. b) revisión periódica del contenido de los campos clave o los archivos de datos para confirmar su validez e integridad.	La Central de Riesgo deberá validar los datos de entrada a las aplicaciones del sistema para garantizar su correctitud. Deberá hacerse una revisión periódica de los mismo.	Sí	La Central de Riesgo debera revisar periódicamente los parámetros necesarios para el funcionamiento de sus aplicaciones de manera que estas adopten la realidad a la cual está circunscrita la organización. Estos parámetros serán mantenidos por un encargado y es el quién deberá velar por la correctitud de los mismos.
			Falta de procedimiento formal para el registro y retiro del registro de usuario											
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos	IDR91	Debido a la falta de autentificación personal no autorizado acceda al aplicativo y se produzcan ataques a la aplicación	4	4	7					
			Gestión deficiente de las contraseñas											
			Uso incorrecto de software	Error en el uso										
A44	Generar Servicios Etapa Prospección	Aplicación Georeferenciada	Distribución errada de los derechos de acceso	Abuso de los derechos	IDR92	Debido a la falta de pruebas en el software traiga como consecuencia una inadecuada gestión de accesos y se otorguen mayores accesos a los usuarios de los que se definieron inicialmente, posibilitando el uso incorrecto de los mismos.	4	4	7					
			Falta de documentación y actualización de dicha documentación	Error en el uso										
			Configuración incorrecta de parámetros											
			Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos										
			Gestión deficiente de las contraseñas											

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A46	Generar Servicios Etapa Prospección	Manual de uso de Aplicación para generar Modelos Estadísticos	Falta de políticas para la utilización de activos de la empresa	Error en el uso	IDR114	Por fallas en la gestión (almacenamiento) de la documentación (manuales, procedimientos, reporte de turnos e indicadores de gestión), esta no se encuentre disponible o pueda ser accedido por personal no autorizado, facilitando su copia a hurto	4	3	6	12.1.1	Todos los activos deben estar claramente identificados y un inventario de todos los activos importantes elaborado y mantenido.	El Central de Riesgo deberá establecer una clasificación para la información y su asociación con las instalaciones de precesamiento de información.	Sí	Actualmente el Central de Riesgo cuenta con algunas tipificaciones de información. Debe establecer una clasificación para la inormación de manera que sea valida para toda la organización y de esta forma poder respetar la clasificación en cada instalción que esta sea procesada.
				Hurto del manual o copias ilegales										
			Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Copiado del software o el manual										
A47	Generar Servicios Etapa Prospección	Manual de uso de Aplicación Aplicación Georeferenciada	Falta de políticas para la utilización de activos de la empresa	Error en el uso	IDR115	Por fallas en la gestión (almacenamiento) de la documentación (manuales, procedimientos, reporte de turnos e indicadores de gestión), esta no se encuentre disponible o pueda ser accedido por personal no autorizado, facilitando su copia a hurto	4	3	6					
				Hurto del manual o copias ilegales										
			Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Copiado del software o el manual										
			Entrenamiento insuficiente en seguridad	Error en el uso										
A57	Generar Servicios Etapa Recuperación	Paquetes de Cartas de Cobranza	Trabajo no supervisado del personal externo o de limpieza	Hurto de los paquetes	IDR127	Por inadecuadas políticas de acceso, personal no autorizado tenga acceso a información confidencial para el negocio , pudiendo afectar la integridad y/o disponibilidad de la información.	4	3	6	8.1.3	Todos los activos deben estar claramente identificados y un inventario de todos los activos importantes elaborado y mantenido.	El Central de Riesgo deberá establecer una clasificación para la información y su asociación con las instalaciones de precesamiento de información.	Sí	Actualmente el Central de Riesgo cuenta con algunas tipificaciones de información. Debe establecer una clasificación para la inormación de manera que sea valida para toda la organización y de esta forma poder respetar la clasificación en cada instalción que esta sea procesada.
			Falta de procedimientos para el manejo de información clasificada	Error en el uso										
			Falta de control de los activos que se encuentran fuera de las instalaciones	Hurto de los paquetes										

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A58	Generar Servicios Etapa Recuperación	Courier	Trabajo no supervisado de personal externo	Hurto de los documentos o paquetes	IDR 135	Por inadecuadas políticas de acceso (por ejem: fallas en custodia de documentos) personal externo tenga acceso a equipos o documentación que almacenan o procesan información crítica para el negocio del Banco, pudiendo afectar la integridad y/o disponibilidad de la información.	4	3	6	9.1.1	Medios físicos en tránsito: e) deberían adoptarse controles especiales para proteger la información sensible de la divulgación o modificación no autorizadas, por ejemplo, envase con detección de apertura (que revela cualquier intento de acceso).	La Central de Riesgo deberá proteger la información en medios físicos en tránsito (durante el envío a las distintas sedes) mediante algún control para evitar su divulgación o modificación no autorizada.	Sí	La Central de Riesgo podría establecer el envío de la información (en este caso los exámenes) mediante paquetes especiales que sean diferenciados y estén sellados, de manera que cualquier intento se acceso a esta pueda ser identificado.
			Falta de conciencia acerca de la seguridad	Error en el uso										
			Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con terceros	Abuso de los derechos										
			Falta de procedimientos para el manejo de información clasificada	Error en el uso										
			Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de activo										
A59	Generar Servicios Etapa Recuperación	Cargo	Entrenamiento insuficiente en seguridad	Error en el uso	IDR 136	Debido a que el personal (en especial los couriers) desconozcan las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	4	3	6	7.2.2	Políticas y procedimientos para el intercambio de información y software: Se deberían establecer políticas, procedimientos y controles formales de intercambio con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación. a) los procedimientos designados para proteger la información intercambiada de una intercepción, copiado, modificación, cambio de ruta y destrucción;	La Central de Riesgo debe establecer un procedimiento formal de intercambio de información que con el fin de proteger la información durante el intercambio de la misma.	Sí	El centro debería tener identificada la información en todo momento y saber donde se encuentra y quien accede a esta. Para este caso se encontró que las fchas con el nivel del alumno están expuestas a modificaciones y por ende podrían ser ingresadas como data corrupta al sistema. Por estos motivos se debe establecer el procedimiento de intercambio de información durante este proceso de manera que se evite estás exposiciones inseguras.
			Trabajo no supervisado del personal externo o de limpieza	Hurto de los paquetes										
			Falta de procedimientos para el manejo de información clasificada	Error en el uso										
			Falta de control de los activos que se encuentran fuera de las instalaciones	Hurto de los paquetes										

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A60	Generar Servicios Etapa Recuperación	Equipo móvil	Susceptibilidad a la humedad, el polvo y la suciedad. Falta de cuidado en la disposición final Uso incorrecto de software y hardware Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Destrucción del equipo. Polvo, corrosión, congelamiento Hurto de equipo Error en el uso Uso no autorizado del equipo	IDR137	Debido a falta de capacitaciones a empleados en seguridad y empleo de activos, se dañen o roben.	4	4	7	6.2.1	Una política formal debe estar en su lugar, y las medidas de seguridad apropiadas deben ser adoptadas para proteger contra los riesgos del uso de la informática móvil y medios de comunicación.	El Central de Riesgo deberá vigilar las condiciones ambientales, como temperatura y humedad, que puedan afectar negativamente al funcionamiento de los equipos en los cuales se da tratamiento o es almacenada la información.	Sí	Se deberá averiguar sobre las condiciones físicas pertinentes al lugar en el cual está la sede del Central de Riesgo. Determinar y acondicionar un área en la cual se pueda asegurar la integridad física de los equipos de tratamiento de información.
A61	Generar Servicios Etapa Recuperación / Generar Servicios Etapa Admisión	Aplicación B2B	Defectos bien conocidos en el software Falta de mecanismos de identificación y autentificación, como la autentificación de usuario Tablas de contraseñas sin protección	Abuso de los derechos Falsificación de derechos	IDR138	Debido a fallas en la aplicación no se llegue a brindar el servicio	4	3	6	6.2.2	Uso de contraseñas: Los usuarios deberían seguir buenas prácticas de seguridad para la selección y uso de sus contraseñas. Mantener la confidencialidad de las contraseñas.	La Central de Riesgo debe difundir las buenas prácticas de seguridad para el trato que se le dan a las contraseñas asignadas.	Sí	La Central de Riesgo deberá establecer y difundir a sus empleadores medidas con las cuales se asegure la confidencialidad de las contraseñas otorgadas.
A62	Generar Servicios Etapa Recuperación	Servidor FTP	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario cifrados	Falsificación de derechos Corrupción de datos Hurto de información	IDR139	Por inadecuadas políticas de acceso personal no autorizado tenga acceso a pudiendo afectar la integridad y/o disponibilidad de la información.	4	4	7	11.2.6	Mantenimiento de equipos: Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad. Los equipos se deberían mantener de acuerdo a las recomendaciones de intervalos y especificaciones de servicio del suministrador.	La Central de Riesgo deberá encargarse de mantener adecuadamente los equipos de acuerdo a las indicaciones de los proveedores para asegurar su continua disponibilidad e integridad.	Sí	La Central de Riesgo deberá seguir lo detallado en los manuales de los equipos para poder cumplir con el mantenimiento de los mismos y esporádicamente contratar servicios de mantenimiento siempre y cuando sea necesario.

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A64	Generar Servicios Etapa Admisión	Verificadores	Uso incorrecto de los equipos móviles	Error en el uso	IDR170	Por inadecuadas políticas de acceso personal externo tenga acceso a equipos o documentación que almacenan o procesan información crítica para el negocio del Banco, pudiendo afectar la integridad y/o disponibilidad de la información.	5	3	7	7.2.3	Las responsabilidades para llevar a cabo la terminación del empleo o cambio de empleo deben estar claramente definidas y asignadas.	El Central de Riesgo debe identificar, documentar e implementar las reglas para un uso aceptable del correo electrónico.	Sí	Como parte de la educación organizacional que se brinda (de alguna forma) a los trabajadores, el Central de Riesgo deberá indicar las normas claras para el uso del correo electrónico que se les otorga.
				Procesamiento ilegal de datos										
			Falta de capacitación para la realización de sus actividades	Error en el uso de equipo										
			Trabajo no supervisado	Hurto de equipos										
			Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos						8.1.4	Una política de control de acceso debe ser establecido, documentado y revisado sobre la base de los negocios y los requisitos de seguridad para el acceso.	El Central de Riesgo deberá ejercer un entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales a todos los empleados de la organización y donde sea relevante.	Sí	Se deberá encargar a las direcciones del Central de Riesgo dicho entrenamiento de manera que todos los empleados estén al tanto de las dispocisiones realizadas en la organización.
			Falta de proceso formal para la revisión (supervisión) de los derechos de acceso											
			Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los verificadores	Procesamiento ilegal de datos	IDR171	Por falta de capacitación a verificadores se procese información incorrecta o se incumplan normas internas pudiendo generar vulnerabilidades en la seguridad como robo de equipo.	4	5	8					

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A64	Generar Servicios Etapa Admisión	Verificadores	Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo o información	IDR171	Por falta de capacitación a verificadores se procese información incorrecta o se incumplan normas internas pudiendo generar vulnerabilidades en la seguridad como robo de equipo.	4	5	8	7.2.1	Una política de control de acceso debe ser establecido, documentado y revisado sobre la base de los negocios y los requisitos de seguridad para el acceso.	El Central de Riesgo deberá ejercer un entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales a todos los empleados de la organización y donde sea relevante.	Sí	Se deberá encargar a las direcciones del Central de Riesgo dicho entrenamiento de manera que todos los empleados estén al tanto de las dispocisiones realizadas en la organización.
A77	Generar Servicios Etapa Admisión	Aplicación de Verificaciones	Falta o insuficiencia de la prueba del software	Abuso de los derechos	IDR172	Debido a un mal funcionamiento del aplicativo web podrían haber intentos no autorizados de acceso que no sean detectados y se produzcan ataques informáticos, lo que conlleva a robo o fuga de información	5	3	7	9.4.1	Declaraciones de requisitos de negocio para nuevos sistemas de información, o mejoras a los sistemas de información existentes deben especificar los requisitos para los controles de seguridad.	El Central de Riesgo deberá validar los datos de entrada a las aplicaciones del sistema para garantizar su correctitud. Deberá hacerse una revisión periódica de los mismo.	Sí	El Central de Riesgo debera revisar periódicamente los parámetros necesarios para el funcionamiento de sus aplicaciones de manera que estas adopten la realidad a la cual está circunscrita la organización. Estos parámetros serán mantenidos por un encargado y es el quién deberá velar por la correctitud de los mismos.
			Falta de control eficaz del cambio											
			Falta de procedimiento formal para el registro y retiro del registro de usuario	Abuso de los derechos	IDR175	Debido a la falta de mecanismos de autenticación e identificación de usuarios / logs insuficientes, no sea posible identificar a usuario y por ende no sea posible tomar acción correctiva.	5	2	6					
A59	Generar Servicios Etapa Admisión	Cargo Verificaciones	Entrenamiento insuficiente en seguridad	Error en el uso	IDR194	Debido a que el personal (en especial los couriers) desconozcan las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	4	3	6	9.1.1	Medios físicos en tránsito: e) deberían adoptarse controles especiales para proteger la información sensible de la divulgación o modificación no autorizadas, por ejemplo, envase con detección de apertura (que revela cualquier intento de acceso).	La Central de Riesgo deberá proteger la información en medios físicos en tránsito (durante el envío a las distintas sedes) mediante algún control para evitar su divulgación o modificación no autorizada.	Sí	La Central de Riesgo podría establecer el envío de la información (en este caso los exámenes) mediante paquetes especiales que sean diferenciados y estén sellados, de manera que cualquier intento se acceso a esta pueda ser identificado.
			Trabajo no supervisado del personal externo o de limpieza	Hurto de los paquetes										
			Falta de procedimientos para el manejo de información clasificada	Error en el uso										
			Falta de control de los activos que se encuentran fuera de las instalaciones	Hurto de los paquetes										

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A65	Comprar Información	Contrato Proveedores	Falta de revisiones en las disposiciones por parte de la gerencia	Usos no autorizados de hardware y software Hurto de equipos, documentos o/y información Abuso de los derechos	IDR292	Debido a una falta de revisión de las disposiciones en los contratos con las fuentes, no se establezcan medidas de seguridad para con los clientes, generando fraudes ,y/o hurto de información o equipos sin la posibilidad de recibir una indemnización por la pérdida financiera generada	5	3	7	15.2.2	Los roles y responsabilidades de seguridad de los empleados y terceras partes deben ser definidos y documentados de acuerdo con la política de información de la organización de seguridad.	El Central de Riesgo deberá establecer una clasificación para la información y su asociación con las instalaciones de precesamiento de información.	Sí	Actualmente el Central de Riesgo cuenta con algunas tipificaciones de información. Debe establecer una clasificación para la inormación de manera que sea valida para toda la organización y de esta forma poder respetar la clasificación en cada instalción que esta sea procesada.
A67	Comprar Información	Cintas magnéticas - Back ups	Falta de esquemas de reemplazo periódico. Susceptibilidad a la humedad, el polvo y la suciedad.	Destrucción de los medios. Polvo, corrosión, congelamiento	IDR293	Debido a una inadecuada gestión de los accesos , personal no autorizado pueda acceder a las oficinas de Adquisición de Datos y pueda provocar daños a equipos y robo de medios de almacenamiento	4	4	7	12.3.1	Medios físicos en tránsito: e) deberían adoptarse controles especiales para proteger la información sensible de la divulgación o modificación no autorizadas, por ejemplo, envase con detección de apertura (que revela cualquier intento de acceso).	La Central de Riesgo deberá proteger la información en medios físicos en tránsito (durante el envío a las distintas sedes) mediante algún control para evitar su divulgación o modificación no autorizada.	Sí	La Central de Riesgo podría establecer el envío de la información (en este caso los exámenes) mediante paquetes especiales que sean diferenciados y estén sellados, de manera que cualquier intento se acceso a esta pueda ser identificado.
			Almacenamiento sin protección Copia no controlada	Hurto de medios							Copias de seguridad de la información y el software deben ser tomadas y analizadas periódicamente de acuerdo con la política de copia de seguridad de acuerdo.	El Central de Riesgo debe identificar, documentar e implementar las reglas para un uso aceptable del correo electrónico.	Sí	Como parte de la educación organizacional que se brinda (de alguna forma) a los trabajadores, el Central de Riesgo deberá indicar las normas claras para el uso del correo electrónico que se les otorga.
A79	Comprar Información	Personal Legal	Entrenamiento insuficiente en seguridad	Error en el uso de aplicaciones	IDR294	Por incumplimiento de procedimientos, se produzcan ataques informáticos a aplicaciones del negocio, o a equipos como servidores pudiendo provocar indisponibilidad y/o falta de integridad de las aplicaciones e información de Titulares	5	4	8	7.2.2	La política de seguridad de la información debe ser revisado a intervalos planeados o si ocurren cambios significativos para asegurarse de su conveniencia, adecuación y eficacia.	Se deberán elaborar guías de clasificación de la información en base a distintos aspectos de manera que se pueda asegurar la pretección de la misma.	Sí	Actualmente el Central de Riesgo cuenta con algunas tipificaciones de información. Debe establecer una clasificación para la inormación de manera que sea valida para toda la organización y de esta forma poder respetar la clasificación en cada instalción que esta sea procesada.

ID	Proceso/s por Activo	Activo	Vulnerabilidad	Amenaza	IDR	Riesgo Identificado	Impacto	Probabilidad de Ocurrencia	Valor	Control	Detalle	Adaptación al caso	Aplicable	Justificación
A80	Comprar Información	Personal Adquisición de información	Entrenamiento insuficiente en seguridad Falta de mecanismos de monitoreo	Error en el uso de aplicaciones Procesamiento ilegal de los datos	IDR295	Debido a que el personal desconozca las normas, políticas y criterios de seguridad de información, se incumplan las normas internos pudiendo generar debilidades y vulnerabilidades de seguridad.	5	4	8	7.2.2	La política de seguridad de la información debe ser revisado a intervalos planeados o si ocurren cambios significativos para asegurarse de su conveniencia, adecuación y eficacia.	Se deberán elaborar guías de clasificación de la información en base a distintos aspectos de manera que se pueda asegurar la pretección de la misma.	Sí	Actualmente el Central de Riesgo cuenta con algunas tipificaciones de información. Debe establecer una clasificación para la inormación de manera que sea valida para toda la organización y de esta forma poder respetar la clasificación en cada instalción que esta sea procesada.
A82	Comprar Información	Personal Control de Calidad	Uso incorrecto de software y hardware	Error en el uso	IDR296	Debido a que personal no tenga el conocimiento suficiente para la utilización de aplicaciones o hw y a falta de monitorio, se presenten errores o ingreso ilegal de data.	4	3	6					
A86	Comprar Información	Puertas de entrada a las Oficinas	Falta de protección física de las puertas, falta de mecanismo de autentificación	Hurto de equipos o información	IDR297	Debido a inadecuadas políticas de seguridad para el acceso físico al edificio, personal no autorizado tenga acceso a equipos que almacenan o procesan información crítica para el negocio del Banco, pudiendo afectar la integridad y/o disponibilidad de la información.	5	3	7	11.1.2	Las áreas seguras deberían estar protegidos por controles de entrada (como tarjetas electrónicas) adecuados para garantizar que sólo se autoriza personal se les permite el acceso.	El Central de Riesgo deberá minimalizar las indicaciones del propósito de sus oficinas, sin signos obvios, fuera o dentro del edificio, que identifiquen la presencia de actividades de tratamiento de información en ellas.	Sí	Se deberá evaluar todas la simbología establecida en las instalaciones y distintas sedes del Central de Riesgo a medida que se determine el propósito de cada símbolo y se pueda retirar lo que sea inadecuado.
A66	Comprar Información	Aplicación utilizada en el proceso de adquisición	Falta o insuficiencia de la prueba del software Defectos bien conocidos en el software Falta de pruebas de auditoría Distribución errada de los derechos de acceso	Abuso de los derechos	IDR311	Debido a fallas en el proceso de definición de roles, algunos puestos de trabajo tengan accesos restringidos o amplios accesos, posibilitando el uso inadecuado de los mismos o limitando las funciones del puesto.	5	3	7	9.4.3	Procedimientos de manipulación de la información: Los procedimientos para la manipulación y almacenamiento de la información deben ser establecidos para proteger esta información de divulgaciones o usos no autorizados. Restricciones de acceso para identificar al personal no autorizado.	La Central de Riesgo debe definir un procedimiento claro para el manejo de sus activos de información durante sus procesos y de esta forma asegurar que esten protegidos y evitar el aceso de peronas no autorizadas a estos.	Sí	La Central de Riesgo deberá analizar los procesos afectados y de esta manera corregir las deficiencias encontradas (ausencia de personal) que podrían acpntecer con incidencias de seguridad.

Mapeo con COBIT 5

Control	Detalle	Proceso Cobit 5
12.3.1	Procedimientos de manipulación de la información: Los procedimientos para la manipulación y almacenamiento de la información deben ser establecidos para proteger esta información de divulgaciones o usos no autorizados. Restricciones de acceso para identificar al personal no autorizado.	DSS06 - Administrar los controles de los procesos claves del negocio
12.1.2	Sesiones inactivas deben cerrar después de un período definido de inactividad.	BAI06 Gestión de cambios
14.2.2	Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal, y una técnica de autenticación adecuado debe ser elegido para demostrar la identidad alegada de un usuario.	
9.4.1	El acceso a la información y funciones de la aplicación del sistema por los usuarios y personal de apoyo deben limitarse de acuerdo con la política de control de acceso definidas.	BAI02 Gestión en la definición
9.4.3	Gestión de contraseñas de usuario: Se debería controlar la asignación de contraseñas por medio de un proceso de gestión formal. a) requerir que los usuarios firmen un compromiso para mantener en secreto sus contraseñas personales y las compartidas por un grupo sólo entre los miembros de ese grupo.	BAI10 Administrar la configuración
8.1.2	La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares a través de un proceso formal.	BAI09 Gestión de activos
18.1.1	Un proceso de autorización de la administración para las nuevas instalaciones de procesamiento de información debe ser definida e implementada.	MEA03 Monitorear y evaluar el cumplimiento de requerimientos externos.
8.1.3	Los usuarios deben asegurarse de que el equipo desatendido tiene la protección adecuada.	BAI09 Gestión de Activos
8.1.1	Todos los activos deben estar claramente identificados y un inventario de todos los activos importantes elaborado y mantenido.	
13.2.1	Información involucrada en las transacciones en línea debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración mensaje no autorizada, revelación no autorizada, mensaje no autorizado, duplicación o repetición.	MEA01 Monitor, evaluate and assess performance and conformance

Control	Detalle	Proceso Cobit 5
13.1.1	Información involucrada en las transacciones en línea debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración mensaje no autorizada, revelación no autorizada, mensaje no autorizado, duplicación o repetición.	DSS06 Manage business process controls
8.1.4	Normas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de información deben ser identificados, documentados e implementados.	BAI09 Manage assets
13.2.3	Information involved in electronic messaging should be appropriately protected.	DSS06 Manage business process controls
12.5.1	Instalación y protección de equipos: f) se deberían vigilar las condiciones ambientales, como temperatura y humedad, que puedan afectar negativamente al funcionamiento de los equipos de tratamiento de información	BAI07 Manage change acceptance and transitioning
9.4.5	El accesos al código fuente debe ser restringido	
11..2.6	Toda la información y los activos asociados con las instalaciones de procesamiento de información deben ser propiedad de una parte determinada de la organización.	AI09 Manage assets
15.1.1	Acuerdos con terceros relacionados con el acceso, tratamiento, comunicación o gestión de la información de la organización o las instalaciones de procesamiento de información, o la adición de productos o servicios a instalaciones de procesamiento de información debe cubrir todos los requisitos de seguridad pertinentes.	MEA02 Monitor, evaluate and assess the system of internal control

Control	Detalle	Proceso Cobit 5
15.2.1	La verificación de antecedentes en todos los candidatos debe llevarse a cabo de acuerdo con las leyes, regulaciones y ética, y proporcional a los requerimientos del negocio, a la clasificación de la información que se accede, y a los riesgos percibidos.	APO10 Manage suppliers
15.2.2	Políticas y procedimientos para el intercambio de información y software: Se deberían establecer políticas, procedimientos y controles formales de intercambio con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación. a) los procedimientos designados para proteger la información intercambiada de una intercepción	
15.2.2	Los roles y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceras partes deben ser definidas y documentadas, de conformidad con la política de información de la organización de seguridad.	
16.1.5	Eventos seguridad de la información debe ser reportada a través de canales de gestión adecuadas tan pronto como sea posible.	APO12 Manage risk
14.1.1	Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollado e implementado.	BAI02 Manage requirements definition
12.1.2	Una política de control de acceso debe ser establecida, documentada y revisada sobre la base de los negocios y los requisitos de seguridad para el acceso.	BAI10 Manage configuration
12.1.4	La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares a través de un proceso formal.	

Control	Detalle	Proceso Cobit 5
15.1.1	Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes a las instalaciones de procesamiento de información y la información deben ser retirados a la terminación de su empleo, contrato o acuerdo, o ajustarse a los cambios.	DSS06 Manage business process controls
12.7.1	Registro de la auditoria: Los registros de auditoria grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados para un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso.	MEA01 Monitor, evaluate and assess performance and conformance
12.6.1	Restricción de acceso a la información: Se debería dar acceso a la información y a las funciones del sistema de aplicaciones sólo a los usuarios de éste, incluido el personal de apoyo, de acuerdo con una política de control de accesos definida.	BAI02 Manage requirements definition
11.1.4	Instalación y protección de equipos: f) se deberían vigilar las condiciones ambientales, como temperatura y humedad, que puedan afectar negativamente al funcionamiento de los equipos de tratamiento de información	BAI09 Manage assets
12.1.2	Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal, y una técnica de autenticación adecuado debe ser elegido para demostrar la identidad alegada de un usuario.	BAI06 Manage changes
14.2.9	Gestión de la aceptación del cambio y de la Transición	BAI07 Manage change acceptance and transitioning