PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

RIESGO	TIPO DE RIESGO	Activo(s) afectados	VULNERABILIDAD	AMENAZA	PLAN DE TRATAMIENTO
Modificación no autorizada de la información	Integridad	Bases de Datos	Falta de políticas que rigen el uso aceptable de los activos de información Asignación errada de los derechos de acceso Ausencia de mecanismos de identificación y autentificación Ausencia de mecanismos de monitoreo Ausencia de procedimientos para el manejo de información tipificada Ausencia de control de los activos que se encuentran fuera de las instalaciones Mantemiento insuficiente Exposición de datos de respaldo Vulnerabilidades conocidas Gestión deficiente de credenciales de acceso Información legible y en texto plano	Incumplimiento en el mantenimiento Ataque informático Abuso de derechos Falsificación de derechos Sabotaje de la información Suplantación de identidad	Establecer directrices sobre el buen uso de la información en las bases de datos. 1. El acceso y diferentes acciones en las bases de datos debería contemplar configuraciones tipo RBAC, que controlen Roles y Privilegios para cada uno de los usuarios y administradores.(Servidores AAA) 2. Las bases de datos deberán generar y mantener una trazabilidad sobre todas las acciones realizadas sobre las mismas. 3. Deberá clasificarse la información que pueda existir dentro de las bases de datos, teniendo en cuenta su criticidad. 4. Detallar adecuadamente los procedimientos que se realizan en las bases de datos. 5. Realizar pruebas de vulnerabilidad o pentesting periódicas al (los) motores de bases de datos y aplicar los diferentes parches de seguridad, teniendo en cuenta las posibles consecuencias en la funcionalidad de los aplicativos. 6. Cifrar adecuadamente la información respaldada en soluciones NAS o en cintas, existen soluciones de almacenamiento con estas características. 7. Evitar emplear aplicaciones/códigos/componentes, que tengan vulnerabilidades conocidas en fuentes como (CVE, NVD) entre otras fuentes. 8. Definir una política de contraseñas seguras, que rijan todos los accesos a las bases de datos, si se considera necesario, se deberá implementar 2 o más factores de autenticación. 9. Definir planes de mantenimiento/depuración/actualización/afinamiento de las bases de datos de manera periódica. 10. Todas las bases de datos deberán ser tenidas en cuenta para la generación de las políticas y planes de respaldos de información. 11. Las bases de datos deberán estar debidamente cifradas y protegidas contra escritura no autorizada, empleando los algoritmos/herramientas necesarias. 12. Tener en cuenta el TOP 10 de vulnerabilidades de OWASP, para proteger las bases de datos.
		Información en transito (correos electrónicos, Drive, página web, carpetas compartidas, dispostivos de almacenamiento)	Falta de políticas que rigen el uso aceptable de los activos de información Ausencia de pruebas de envío o recepción de mensajes Líneas de comunicación sin protección Tráfico sensible sin protección Ausencia de mecanismos de monitoreo Ausencia de identificación y auntenticación de emisor y recepto Conexiones de red publicas sin protección Gestion inadecuada de la red (Tolerancia a fallos en el enrutamiento)	Escucha encubierta Espionaje remoto Incumplimiento en el mantenimiento Ataque informático Suplantación de identidad	Teniendo en cuenta las conexiones de red que se definan y que así lo requieran, se deberán implementar las siguientes medidas: Para las conexiones entre entidades es importante tener en cuenta las siguientes recomendaciones: 1. Los canales de información que tengan como medio de transmisión internet, deberán emplear el uso de tecnologías como VPN, para garantizar la integridad y la confidencialidad de la información que está siendo transmitida. 2. Monitorear los canales y las conexiones, para verificar posibles pérdidas en el canal que puedan afectar los datos transmitidos. 3. Para las conexiones de enrolamiento (que utilizarán internet), un tipo de acceso distinto a la solución de servicios digitales básicos, se recomienda el uso de VPN tipo Client-to-Site, que permita que puedan unirse a la red donde está implementada la solución y poder realizar los enrolamientos o registros de nuevos usuarios. 4. Los accesos a las plataformas deberán tener diferentes factores de autenticación si así se consideran, teniendo una política de contraseñas previamente definida en los sistemas de información. 5. Aplicación de defensa en profundidad, es decir, un perímetro de acceso a los sistemas a través de sistemas como firewalls stateful y de capa de aplicación, Intrusion Prevention Systems y Proxy, definición de VLANs (Segmentación de Red), restricciones a través de ACL (Access Control List) cuando sea conveniente y implementación de honeypots. 6. Al compartir información a través de Drive, se deben establecer permisos solamente de descarga y a correos puntuales (Conocidos). NOTA: Para cifrado a nivel de red, se recomendaría el uso del protocolo IPSEC con ESP (Encapsulating Security Protection), que busca el cifrado del canal o tunel VPN y de la información que viaje a través de este). Debe emplearse para cifrado de VPN a nivel web, el protocolo TLS, SSL está obsoleto y tiene graves vulnerabilidades conocidas.
		front End Usuarios, Front End Operador Front End Entidad	Asignación errada de los derechos de acceso Ausencia de mecanismos de identificación y autentificación Ausencia de mecanismos de monitoreo Ausencia de manuales de uso Mantemiento insuficiente Ausencia o insuficiencia de pruebas Ausencia de terminación de sesión Vulnerabilidades conocidas Gestión deficiente de credenciales de acceso	Incumplimiento en el mantenimiento Ataque informático Abuso de derechos Falsificación de derechos Sabotaje de la información Suplantación de identidad	1. Ejecutar pruebas de pentesting en los diferentes front-ends definidos, con el objetivo de evitar los siguientes tipos de ataques (Considerando que serán páginas web: *Web Parameter Tampering. *XSS (Cross Site Scripting) *SQL Injections +Defacement 2. Implementar el protocolo TLS en su versión más estable en combinación con HTTPS y el certificado correspondiente (con la CA que mejor se considere). 3. Implementar mecanismos de autenticación de diferentes factores para reducir los riesgos de suplantación de identidad. 4. Implementar elementos de seguridad perimetral como firewalls y/o balanceadores para evitar ataques DDoS a las plataformas front-end. 5. Implementación Web Application Firewall. 6. Desarrollar el código de las aplicaciones web teniendo en cuenta las recomendaciones dadas en OWASP,

Pérdida, destrucción o daño de la información	Disponibilidad	Información en transito (correos electrónicos, Drive, página web, carpetas compartidas, dispostivos de almacenamiento)	* Procedimientos o políticas ausentes o definidas deficientemente * Servicio de energía eléctrica inestable * Inexistencia de protección contra inundaciones * Infraestructuras física inadecuadas o en mal estado, no resistente a desastres naturales * Protección física insuficiente o incorrecta * Insuficiente acondicionamiento de aire (altas temperaturas) * Falta de capacidades y competencias * Falta de conciencia seguridad de la información * Medios de comunicación y equipos obsoletos o en mal estado. * Exposición a humedad, contaminación, electromagnetismo * Inexistencia de contingencia * Programación o configuración insegura * Vulnerabilidad de las plataformas y protocolos de la Base de Datos * Ataques por intrusos o inyección SQL * Exposición de los Datos Backups * Missing Function Level Access * Ausencia de políticas y recursos de backup/respaldo * Falta o débil control de acceso físico y lógico	Terremoto Incendio Robo de Información Terrorismo Falla en equipo de telecomunicaciones Ataque informatico	1. Verificar canales de contingencia entre los operadores, para evitar perdida de solicitudes de transacciones o transmisión de información entre los mismos. 2. Elaborar un plan de continuidad de negocio, con roles, responsabilidades, recursos tecnológicos y personal necesario para asegurar la continuidad del servicio en los escenarios más críticos. 3. Disponer de dos datacenters con las siguientes condiciones mínimas: *Datacenter principal, que mínimo cumpla las condficiones/configuraciones TIER3. *Datacenter alterno (ubicado geográficamente en otro sitio) y que permita a su vez mitigar las amenazas de tipo natural y de terrorismo. que mínimo cumpla con configuraciones TIER2. 4. Todos los procedimientos de contingencia deberán estar debidamente documentados, para garantizar una respuesta adecuada ante posibles incidentes y a su vez la mayor disponibilidad posible de los servicios y de la información. 5. Mantener mantenimiento y monitoreo constante en los sistemas de refrigeración y de control de humedad.6. Control de acceso físico a datacenters, con registros (preferiblemente bajo sistemas de información) 7. Capacitar al personal de seguridad física, en temas de seguridad de la información. 8. Implementar sistemas DLP (Data Leak Prevention), a nivel de redes, para evitar fugas de información sensible.
		Información en reposo		Terremoto Incendio Falla en el suministro de energía Robo de Información Terrorismo Falla en equipos de respaldo Falla en equipos de telecomunicaciones Ataque informatico Error humano	1. Elaborar un plan de continuidad de negocio, con roles, responsabilidades, recursos tecnológicos y personal necesario para asegurar la continuidad del servicio en los escenarios más críticos. 2. Disponer de dos datacenters con las siguientes condiciones mínimas: *Datacenter principal, que mínimo cumpla las condficiones/configuraciones por lo menos TIER3. *Datacenter alterno (ubicado geográficamente en otro sitio) y que permita a su vez mitigar las amenazas de tipo natural y de terrorismo. que mínimo cumpla con configuraciones TIER2. 3. realizar mantenimientos periódicos a los sistemas eléctricos, con el diseño de su respectiva contingencia. 4. Mantener mantenimiento y monitoreo constante en los sistemas de refrigeración y de control de humedad. 5. Garantizar protecciones y sistemas contra fuego y explosiones. 6. Puertas y camaras de seguridad en los centros de computo donde se encuentren los componentes que conforman la solución tecnológica.7.Control de acceso físico a datacenters, con registros (preferiblemente bajo sistemas de información) 8. Capacitar al personal de seguridad física, en temas de seguridad de la información. 9. Establecer ambientes adecuados de desarrollo, pruebas y producción para los sistemas de información. 10. Definir políticas de respaldo de información.
Indisponibilidad de la información	Disponibilidad	Información, hardware, software, red	* Using Components with Known Vulnerabilities * Missing Function Level Access * Security Misconfiguration * Insecure Direct Object References * Cross-Site Scriting (XSS) * Injection * Vulnerabilidad de las plataformas y protocolos de la Base de Datos * Software desactualizado / programación insegura * Configuración o instalación incorrectas (puertos abiertos innecesarios, protocolos innecesarios) * Firmware desactualizado * Hardware obsoleto * Exposición a electromagnetismo o temperaturas no toleradas por el HW * Servicio de energía eléctrica inestable * No segmentación de la red * Medios físicos de comunicación obsoletos o en mal estado. * Falta de administración y monitoreo de vulnerabilidades. *Personal Insuficiente / definición incorrecta de roles * Procedimientos o políticas ausentes o definidas deficientemente * Insuficiente acondicionamiento de aire (altas temperaturas)	Terremoto Inmundaciones Derrumbe Sabotaje Terrorismo Falla suministro de energía Falla de telecomunicaciones Falla en hardware Falla en software Ataque informatico Incumplimiento en Mantenimiento	1. Definir una política de continuidad de negocio y los respectivos planes derivados para los servicios más críticos. 2. Deberán documentarse todos los procedimientos definidos para la recuperación de los servicios y para el desarrollo de las actividades más críticas para el servicio. 3. Si así lo define el análisis respectivo, deberá implementarse un datacenter alterno, para restaurar los servicios en caso de alguna amenaza de tipo natural (terremoto, inundaciones), un incendio, terrorismo entre otros que pueda afectar físicamente los servicios alojados en el sitio original. 4. Mantener mantenimiento y monitoreo constante en los sistemas de refrigeración y de control de humedad. 5. Entrenar adecuadamente al personal que administra o gestiona la solución, adicionalmente, implementar metodologías de transversalidad, para que la mayoría de los ingenieros conozcan varios temas y puedan suplir bajar de personal de manera temporal. 6. Realizar controles de cambios para verificar consecuencias en actualizaciones o configuraciones nuevas, empleando los respectivos ambientes de desarrollo, pruebas y producción. 7. Implementación de sistemas de seguridad perimetral (IPS, Firewall) y balanceadores, que eviten saturaciones y/o ataques de DDoS. 8. Garantizar pruebas periódicas en contingencia de energía eléctrica, con el uso de UPS, plantas alternas etc.... 9. Garantizar la seguridad física donde se encuentren ubicados los sistemas de información, así mismo asegurar las conexiones electricas para evitar sabotajes como desconexión de los servidores o de los dispositivos de red. 10. Definir tiempos específicos de respuesta y recuperación para los incidentes (ANS), adicionales a los que planamente hablen sobre disponibilidad del servicio.11. Implementación de aplicaciones de seguridad (Antimalware, antiphishing, antispyware, etc.) 12. Disponer de dos datacenters con las siguientes condiciones mínimas: *Datacenter principal, que mínimo cumpla las condficiones/configuraciones por lo menos TIER3. *Datacenter alterno (ubicado geográficamente en otro sitio) y que permita a su vez mitigar las amenazas de tipo natural y de terrorismo. que mínimo cumpla con configuraciones TIER2.
Hurto por parte de propios o terceros	Disponibilidad	Hardware e Información	Ausencia de controles de seguridad fisica Falta de políticas que rigen el uso aceptable de los activos de información Procedimientos ausentes o definidas deficientemente Falta de capacitación en el uso de los aplicativos Falta de sensibilización en seguridad de la información Funcionario insatisfecho Equipos de computo desatentidos	Hurto de equipos Hurto de documentos y/o medios Escucha encubierta Recuperación de medios reciclados o desechados Sabotaje	1. Implementación de soluciones DLP (Data Leak Prevention), tanto a nivel de información en reposo (almacenada), en tránsito o en uso. 2. En el caso de información física sensible, deberá disponerse de un área de archivo con la custodia correspondiente (Puertas, Cámaras de seguridad y Controles de Acceso Físico) 3. Garantizar la seguridad física donde se encuentren ubicados los sistemas de información, así mismo asegurar las conexiones electricas para evitar sabotajes como desconexión de los servidores o de los dispositivos de red. 4. Tener plenamente preparados planes de continuidad de negocio en caso de robo de algún componente específico, teniendo en cuenta los tiempos de respuesta definidos. 5. Políticas para disposición de información de medios físicos. 6. Sensibilización a todo el personal en temas de ingenieria social, para evitar posibles robos de información a través de estos métodos. 7. Implementación de herramientas como antivirus o IPS a nivel de Host, que protejan a los servidores y/o sistemas de información de amenazas como ransomware y otro tipo de malware.

Uso y divulgación no autorizada de información confidencial	Confidencialidad	Información Fisica, Digital	Ausencia de controles de seguridad fisica Falta de políticas que rigen el uso aceptable de los activos de información Procedimientos ausentes o definidas deficientemente Falta de capacitación en el uso de los aplicativos Falta de sensibilización en seguridad de la información Funcionario insatisfecho Equipos de computo desatentidos Asignación errada de los derechos de acceso	Error Humano Sabotaje Acceso no autorizado a instalaciones Conflictos laborales Tratamiento inadecuado de la información Fuga de información	1. Acuerdos de confidencialidad entre los operadores y el Ministerio de Tecnologías de la Información y las Comunicaciones, donde se garantice que la información manipulada por parte de los operadores tiene el único fin de proveer los servicios de carpeta ciudadana al ciudadano y absolutamente nada más, es decir, que esta información no podrá ser utilizada para fines publicitarios ni comerciales, adicionalmente deberán definirse multas y/o sanciones correspondientes si el proveedor del servicio incumple con la protección de los datos que tiene en su poder. 2. Verificación minuciosa sobre el personal contratado (Pasado judicial y pruebas de seguridad), dependiendo del tipo de privilegios que pueda tener en cuanto al acceso a los datos o la información. 3. Firma de acuerdos de confidencialidad para cada uno de los empleados que tengan o no acceso a la información y las instalaciones (incluyendo al personal de mantenimiento y aseo) 4. En los acuerdos o documentos definidos para la confidencialidad, deberá enfatizarse las consecuencias legales y disciplinarias correspondientes en caso de faltar a los compromisos que en este se enuncien. 5. Políticas que regulen el ingreso de dispositivos de almacenamiento extraíbles como discos duros, memorias USB etc... las cuales no deberían emplearse por parte del operador. 6. Limitar el uso de herramientas personales (correo electrónico, soluciones en la nube etc...) Ajenas a las asignadas por el operador, incluyendo los computadores, NO debe haber acceso a la administración de las plataformas desde máquinas particulares o personales. 7. Preparar al personal de técnicas como la ingeniería social para evitar fugas de información por este método. 8. La información sensible o privada que esté alojada en las distintas bases de datos y en las soluciones de respaldo deberán estar debidamente cifradas y protegidas por aplicaciones de seguridad, si existe un robo de la información, no necesariamente implica que la información este legible. 9. Implementación de soluciones DLP (Data Leak Prevention), tanto a nivel de información en reposo (almacenada), en tránsito o en uso. 10. Garantizar la seguridad física donde se encuentren ubicados los sistemas de información, así mismo asegurar las conexiones electricas para evitar sabotajes como desconexión de los servidores o de los dispositivos de red.
Inconsistencias en la información	Integridad	Información, Sistemas de Enrolamiento	* Falta o débil control de acceso físico y lógico * Procedimientos o políticas ausentes o definidas deficientemente * Insuficiente acondicionamiento de aire (altas temperaturas) * Servicio de energía eléctrica inestable * Protocolos de red sin cifrar (transferencias de datos sensibles o críticos en texto plano) * Falta de administración y monitoreo de vulnerabilidades. * Medios físicos de comunicación y equipos obsoletos o en mal estado. * Exposición a electromagnetismo y temperaturas no toleradas por el HW * Falta de mantenimiento * Programación insegura * Vulnerabilidad de la plataforma * Broken Authentication and Session Management * Using Components with Known Vulnerabilities * Cross-Site Request Forgery (CSRF)	Error Humano Sabotaje Conflictos Laborales	1. En los posibles puntos de enrolamiento se recomienda verificar que el personal tenga los procedimientos de enrolamientos bien documentados y definidos. 2. Verificar antecedentes de funcionarios contratados para tal fin. 3. En caso de despido o de bajas de personal, efectuar las bajas en los sistemas de información a la mayor brevedad (esto implica el desarrollo de procedimientos de creación y gestión de usuarios según cada rol). 4. Verificar adecuadamente que los usuarios registren información verídica (incluyendo la biométrica), todo esto en el marco del procedimiento de enrolamiento que deberá generarse. 5. Capacitación adecuada en los diferentes procesos, para evitar el mal uso de las aplicaciones o la carga de información errada en las mismas. 6. Establecimiento de ambientes adecuados de desarrollo, pruebas y producción para los sistemas de información
Acceso no autorizado a la información	Confidencialidad	Información Fisica, Digital, Sistema de Informacion (Bases de Datos), Front-Ends	* Inyección de código * Sensitive Data Exposure * Using Components with Known Vulnerabilities * Unvalidated Redirects and Forwards * Falta o débil control de acceso físico y lógico * Vulnerabilidad de las plataformas y protocolos de la Base de Datos * Abusos de privilegios / elevación de privilegios no autorizada * Vulnerabilidad de las plataformas y exposición de los Datos Backups * Ausencia de filtros ACL entre segmentos de red * No segmentación de la red, puertos abiertos innecesarios y protocolos innecesarios * Robo de credenciales de acceso / uso de contraseñas débiles * Procedimientos o políticas ausentes o definidas deficientemente * Ausencia de Cultura de Seguridad de la Información * Ausencia o deficiencia en roles de acceso a sistemas de información * Falta o débil control de acceso físico y lógico * Fallas en el reclutamiento y definición incorrecta de roles * Falta de conciencia seguridad de la información, capacidades y competencias	Ingenieria Social Escucha Encubierta Espionaje Remoto Ataque informatico Incumplimiento en Mantenimientos Suplantación de Identidad	1. Definición de esquemas AAA para la autenticación, autorización y registro de las transacciones realizadas en los sistemas de información. 2. Definir las políticas de uso aceptable de los recursos tecnológicos asignados, entre ellos la cuentas de usuario de las plataformas de administración. 3. Campañas de sensibilización a la ciudadanía, para que hagan un uso adecuado de las credenciales otorgadas a la solución de servicios digitales básicos. 4. Generación de campañas para la ciudadanía, reforzando los temas principalmente de ingeniería social y phishing, para el robo de datos de acceso. 5. Definir factores adicionales de autenticación que incrementen los niveles de seguridad, teniendo en cuenta los principios: *Algo que el usuario sabe. (Ej. Contraseña, PIN) *Algo que el usuario posee. (Ej. Token, Apps, Tarjetas) *Algo que el usuario es. (Ej .Biometría) *Algo que el usuario sabe hacer. (Ej. Firma) 6. Deberán ejecutarse pruebas de pentesting en los diferentes front-ends y sistemas de información, con el objetivo de evitar los siguientes tipos de ataques (Considerando que serán páginas web: *Web Parameter Tampering. *XSS (Cross Site Scripting). *SQL Injections. 7. Garantizar la seguridad física donde se encuentren ubicados los sistemas de información, así mismo asegurar las conexiones electricas para evitar sabotajes como desconexión de los servidores o de los dispositivos de red. 8. En el caso de información física sensible, deberá disponerse de un área de archivo con la custodia correspondiente (Puertas, Cámaras de seguridad y Controles de Acceso Físico) 9. Implementación de herramientas como antivirus o IPS a nivel de Host, que protejan a los servidores y/o sistemas de información de amenazas de malware que incluyen backdoors, para acceder a los sistemas sin autorización.