Sistema de Remisión de Información de Seguros (SIRISE)

Instructivo para la Remisión de Información de Aseguradoras, Reaseguradoras y Empresas de Tercerización

Versión 1.0

Octubre 2025

Elaborado por:
Superintendencia de Seguros (SIS)

TABLA DE CONTENIDO

INTRODUCCIÓN

El objetivo de este instructivo es guiar a las empresas aseguradoras y reaseguradoras nacionales en el proceso de envío de información obligatoria a través del **Sistema de Remisión de Información de Seguros (SIRISE**) de la Superintendencia de Seguros de la República Dominicana. Este sistema permite monitorear las operaciones del sector, velar por el correcto cumplimiento normativo y proporcionar un nivel adecuado de protección a los usuarios.

Su elaboración se realiza en cumplimiento al Artículo 5 de la Resolución Núm. 01/2024. Este instructivo es de aplicación obligatoria para todas las entidades aseguradoras y reaseguradoras debidamente registradas y autorizadas para operar en la República Dominicana, de conformidad con la Ley Núm. 146-02 sobre Seguros y Fianzas y la Resolución Núm. 01/2024.

Responsabilidad de las Entidades:

- Remisión de información: Es responsabilidad de las aseguradoras, reaseguradoras y empresas de tercerización remitir la información requerida en formato digital, cumpliendo con las frecuencias (diaria, semanal, trimestral o anual) y los plazos establecidos en la resolución 01-2024.
- Integridad de los datos: Deben asegurar que la información generada sea siempre correcta, eficiente y segura, evitando envíos de datos incompletos, inexactos o falsos.

Canales y Plataformas:

Para remitir la información requerida, las entidades supervisadas deben utilizar los canales digitales que la Superintendencia de Seguros habilite. Las opciones disponibles son:

- **Formularios digitales:** para una entrada de datos manual y sencilla a través de una oficina virtual.
- **Archivos de datos:** para el envío de grandes volúmenes de información.
- **Servicios web (APIs):** para una conexión automatizada y directa entre sistemas.
- **Software estadístico:** para el procesamiento y envío de datos complejos.

La Superintendencia indicará a cada empresa el canal más adecuado según su capacidad tecnológica.

En conclusión, la función principal del sistema SIRISE es permitir a la Superintendencia monitorear las operaciones del sector, velar por el correcto cumplimiento de las normativas y proporcionar un nivel adecuado de protección a los usuarios finales.

I. DISPOSICIONES GENERALES

1. Canales de remisión

Las empresas deben remitir la información requerida en formato digital según los plazos establecidos. El proceso de remisión de información se efectuará a través del **Sistema de Remisión de Información de Seguros (SIRISE**), utilizando los siguientes canales digitales:

1.1 Oficina Virtual (Formularios Digitales)

- Dirección de Acceso: https://sis.gob.do/siris/
- Requisitos: Navegador web actualizado.
- Seguridad: Autenticación de usuario.

1.2 FTP (Archivos)

- Dirección de Acceso: Dirección del Servidor, VPN, puerto y protocolo (FTP, SFTP o FTPS)
- Requisitos: Formatos soportados CSV, PDF, EXCEL
- Seguridad: Antivirus, firewall y autenticación.

1.3 Servicios Web (Datos)

- Dirección de Acceso: Servidor base (endpoint) con protocolo HTTPS.
- Requisitos: Datos en formato JSON, XML
- Seguridad: Antivirus, firewall y autenticación

1.4 Plataforma GRC (Datos)

- Dirección de Acceso: Portal de la empresa
- Requisitos: Navegador web o software compatible
- Seguridad: Antivirus, firewall y autenticación

2. Tipos de emisores de información

Son las empresas aseguradoras y reaseguradoras autorizadas por la Superintendencia de Seguros para operar en la República Dominicana y con la obligación de remitir información sobre sus operaciones, conforme a la resolución 01-2024.

2.1 Aseguradoras.

Compañía o sociedad debidamente autorizada para dedicarse exclusivamente a la emisión de contratos de seguros, fianzas y a la contratación de reaseguros y sus actividades consecuentes, de forma directa o a través de intermediarios.

2.2 Reaseguradoras.

Sociedad que, organizada de acuerdo con las leyes de la República Dominicana, autorizada exclusivamente a la contratación de reaseguros y a sus actividades consecuentes.

2.3 Empresas de Tercerización.

Las aseguradoras o reaseguradoras que no dispongan de los medios tecnológicos necesarios podrán contratar a terceros para la remisión de información. Estas empresas de tercerización deben cumplir con los requisitos regulatorios y tecnológicos de la Superintendencia. Funcionaran como intermediarios y emisores de la información, sin asumir de manera directa las responsabilidades que les competen a las entidades aseguradoras en términos de cumplimiento normativo.

Deben utilizar una herramienta estadística GRC para ofrecer visibilidad completa del estado de las operaciones de sus clientes. Una plataforma GRC (software de Gobernanza, Riesgo y Cumplimiento) permite no solo recolectar y remitir datos, sino también generar inteligencia de negocio, analizar riesgos y apoyar la toma de decisiones.

3. Datos a remitir

Las comunicaciones, documentos e informes que deban presentarse firmados podrán ser remitidos en formato digital. Para estos envíos se utilizarán los canales definidos en este instructivo y se aceptará el uso de la firma digital.

El uso del certificado digital para la firma de los documentos es una responsabilidad individual de cada emisor de información, por lo que las aseguradoras, reaseguradoras o empresa de terceros deben poseer sus propios certificados digitales independientemente del canal de remisión que utilicen.

A continuación, se detallan los datos que deben ser remitidos por las entidades.

3.1 Documentos de la Empresa.

- Descripción: Enviar el registro de la empresa, incluyendo:

  1. Certificado de ONAPI
  2. RNC
  3. Estatutos
  4. Registro Mercantil
  5. Listado de suscriptores y actas de asamblea

- Plazo de Remisión: A más tardar 15 días calendario después del 31 de diciembre de cada año.

- Formato: PDF.

3.2 Oficinas, Sucursales y Puntos de venta.

- Descripción: Enviar el listado de todas las oficinas, sucursales y puntos de venta.

- Plazo de Remisión: Mensualmente, a más tardar 15 días luego de finalizado el mes en cuestión.

- Formato: PDF, CSV, JSON, XML

3.3 Funcionarios y Empleados.

- Descripción: Enviar el listado de funcionarios y empleados.

- Plazo de Remisión: Mensualmente, a más tardar 15 días luego de finalizado el mes en cuestión.

- Formato: CSV, JSON, XML

Nota: Todos los documentos generados en formato PDF deben ser firmados digitalmente, salvo otras disposiciones que pueda establecer la Superintendencia.

3.4 Estados Financieros Preliminares.

- Descripción: Enviar los estados financieros utilizando el catálogo de cuentas oficial como referencia.

- Plazo de Remisión:

Mensual: 15 días calendario después del cierre del mes.

Trimestral: 30 días calendario después del cierre del trimestre.

- Formato:CSV, JSON, XML

3.5 Estados Financieros Auditados.

- Descripción: Enviar los estados financieros auditados, utilizando el catálogo de cuentas oficial como referencia.
- Plazo de Remisión: Anual, a más tardar el 30 de abril de cada año, atendiendo a los criterios establecidos en la ley 146-02.
- Formato: CSV, JSON, XML

3.6 Otras Informaciones Adjuntas.

- Descripción: Remitir documentos como listado de inversiones de reservas, listado de cancelaciones de certificados de inversión de la reserva, listado préstamos hipotecarios y listado de préstamos con garantía en las pólizas de vida individual.
- Plazo de Remisión: Mensualmente, a más tardar 15 días luego de finalizado el mes en cuestión.
- Formato: CSV, JSON, XML

3.7 Primas Suscritas por Seguros de Personas.

- Descripción: Remitir la información de las pólizas de seguro suscritas sobre personas, al momento de la suscripción del contrato de la prima.
- Plazo de Remisión: Diariamente, reportándose el primer día laboral de la semana los datos generados en el fin de semana inmediatamente anterior.
- Formato: CSV, JSON, XML

3.8 Primas Suscritas por Seguros Generales y Fianzas.

- Descripción: Remitir información sobre suscripciones de pólizas de incendio y líneas aliadas, vehículos de motor, naves marítimas y aéreas, transporte de carga, agrícola o pecuario, fianzas y otros seguros.

- Plazo de Remisión: Diariamente, reportándose el primer día laboral de la semana los datos generados en el fin de semana inmediatamente anterior.

- Formato: CSV, JSON, XML

3.9 Otras Operaciones de Pólizas.

- Descripción: Remitir información sobre primas cobradas, pólizas canceladas, comisiones pagadas, siniestros reportados, resultado de reclamos y reclamos pagados.

- Plazo de Remisión: Diariamente, reportándose el primer día laboral de la semana los datos generados en el fin de semana inmediatamente anterior.

- Formato: CSV, JSON, XML

3.10 Operaciones de Reaseguro.

- Descripción: Remitir información sobre reaseguros contratados, primas pagadas, siniestros reportados, comisiones pagadas, resultado de reclamos y reclamos cobrados.

- Plazo de Remisión: Diariamente, reportándose el primer día laboral de la semana los datos generados en el fin de semana inmediatamente anterior.

- Formato:CSV, JSON, XML

4. Remisión de Información por la Oficina Virtual

4.1 Llenado de Plantillas

Para conocer la descripción detallada del uso y llenado de las plantillas, consulte el **Manual Para el Registro de Datos en Cumplimiento con la Resolución 01-2024**.

Paso 1: Descargue la plantilla correspondiente al tipo de información que necesita remitir desde el URL https://sis.gob.do/sirise/plantillas/.

Cada plantilla contiene instrucciones para su llenado y carga. Sino hay operaciones que reportar, remita los datos de la plantilla vacía.

Paso 2: Completar la información. Llene el formulario con los datos requeridos para el periodo de trabajo correspondiente.

Paso 3: Procesar la plantilla. Presione el botón PROCESAR para validar y registrar la información. Si el sistema notifica un error, realice la corrección indicada y presione PROCESAR nuevamente hasta que el formulario sea validado correctamente.

IMPORTANTE: Todas las fianzas, pólizas de seguros de personas y generales deben emitirse con firma digital en formato PDF.

4.2 Remitir Información en la Oficina Virtual

Paso 1: Iniciar Sesión. Diríjase a la oficina virtual en https://sis.gob.do/sirise/ovirtual/ e inicie sesión. Si no tiene una cuenta, puede solicitar el registro de su cuenta en el mismo portal.

Paso 2. Seleccionar "Remitir Información" en el menú principal. A continuación, debe seleccionar la opción de Remitir información. En el menú principal, elija la opción para remitir información.

Paso 3. Ingresar Información. Complete los campos requeridos en la pantalla:

Información a remitir:	Seleccione el tipo de información de la lista.
Cargar archivo:	Presione el botón para buscar y seleccionar el archivo generado desde su computador.

Paso 4. Cargar los Archivos. Cargue todos los archivos que necesita remitir. Verifique que aparezcan correctamente en la lista de archivos cargados que detalla el tipo de información, nombre del archivo, fecha y estatus.

Paso 5. Enviar los Datos. Una vez verificado que toda la información es correcta, presione el botón ENVIAR DATOS.

- Un mensaje de éxito confirmará que la remisión se ha completado.
- Si recibe una notificación de error, revise la información, haga las correcciones necesarias y repita el proceso de envío.

Para una mejor compresión del proceso, puede consultar el flujograma.

Figura 1. Flujograma del caso de uso para la remisión de información del SIRISE.

4.3 Reglas de Consistencia y Estandarización

1. **Plantillas**. Utilice siempre la última versión de la plantilla y siga sus instrucciones.

2. **Precisión.** Los datos deben ser precisos y reflejar la realidad. Verifíquelos antes de ingresarlos.
3. **Plazos.** Realice la remisión dentro de los plazos. No se aceptarán un segundos envíos, sin autorización previa.
4. **Formato de Datos.** Sea consistente con los formatos (ej. Fechas como AAAA/MM/DD, texto en mayúsculas/minúsculas de forma uniforme). Especifique y use consistentemente las unidades de medida.
5. **Tipo de Datos.** Asegúrese de usar el tipo de dato esperado (alfanumérico, numérico, fecha, etc.).
6. **Terminología:** Utilice terminología y abreviaturas estándar, siguiente el glosario.
7. **Campos obligatorios:** Complete todos los campos marcados como obligatorios.
8. **Datos faltantes:** La Superintendencia definirá una regla consistente para datos no aplicables (ej. Dejar en blanco, "N/A"). Los campos de fecha no aplicables deben dejarse en blanco.

9. **Nomenclatura de archivos.** Siga el formato estándar para nombrar (ej. NombrePlantilla_Area_Fecha.xlsx)

4.4 Horarios de Remisión

1. **Fechas de remisión:**
   a. Remisiones anuales: A más tardar 15 días calendario luego de concluido cada año observado.
   b. Remisiones trimestrales y mensuales: A más tardar 15 días calendario luego de concluido cada trimestre o mes observado.
   c. Remisiones diarias: Antes de finalizar el día hábil inmediatamente siguiente al día observado.

2. **Días no hábiles:** La información correspondiente a sábados, domingos y días feriados se enviará antes de finalizar el día hábil inmediatamente siguiente.

3. **Cierre de oficinas:** Si la empresa decide no laborar en un día hábil, deberá remitir la información durante el siguiente día hábil y comunicar el cierre a la Superintendencia con al menos tres (3) días hábiles de antelación.

4. **Incumplimiento de Fecha:** Si no puede remitir en la fecha correspondiente, deberá hacerlo posteriormente y notificar las razones a la Superintendencia vía correo electrónico a destudios@sis.gob.do. La Superintendencia, evaluará el caso para determinar si clasifica como no remisión o remisión tardía y aplicará los procedimientos correspondientes.

4.5 Solicitud a la Superintendencia

1. Se realizará antes de las 4:00 p.m. mediante un correo electrónica motivado.

2. Contenido de la Solicitud: La solicitud de reenvío debe incluir:

   a) Identificación de la empresa.
   b) Nombre de las plantillas a reenviar.
   c) Días solicitados para el reenvío.
   d) Justificación del error y detalles de los ajustes realizados.

3. La Superintendencia responderá por correo electrónico habilitando el reenvío, el cual deberá realizarse el mismo día de la autorización.

4.6 Solicitud de Prórroga

1. Requisitos de la Solicitud:

   - Debe ser solicitada mediante comunicación escrita y firmada (física y/o digital) por la máxima autoridad de la empresa. La Superintendencia de Seguros tiene la potestad de aprobar o denegar la prórroga solicitada.

- Debe dirigirse a la máxima autoridad de la Superintendencia, con copia a la Dirección de Estudios del Sector Seguros.

- Debe justificar las razones y listar las plantillas para las cuales se solicita la extensión.

2. Plazos para Solicitar:

   - Remisiones Diarias: A más tardar a las 12 del mediodía del mismo día del vencimiento, en horario laborable.

   - Remisiones Mensuales: Con al menos, cinco (5) días laborables de anticipación.

   - Remisiones Trimestrales o Anuales: Con al menos, diez (10) días laborables de anticipación.

3. Límites y Condiciones:

   Lo límites y las condiciones de las prórrogas están establecidos tanto en la Ley 146-02 como en la Resolución 01-2024, de la siguiente manera:

   - Para la remisión de estados financieros auditados y preliminares trimestrales en formato PDF firmados digitalmente, tendrán la posibilidad de obtener hasta dos (2) prórrogas consecutivas.

   - Para la remisión de las informaciones de corte anual establecidas en la Resolución 01-2024, tendrán la posibilidad de obtener hasta dos (2) prórrogas consecutivas en cada año.

   - Para la remisión de las informaciones de corte mensual establecidas en la Resolución 01-2024, tendrán la posibilidad de obtener hasta dos (2) prórrogas consecutivas en cada mes.

   - Para la remisión de las informaciones de corte diario establecidas en la Resolución 01-2024, tendrán la posibilidad de obtener hasta tres (3) prórrogas en cada mes.

4. Duración máxima de la prórroga:

   Los plazos máximos que puede otorgar la Superintendencia para las solicitudes de prórrogas que esta considere pertinentes son los siguientes:

- Para la remisión de estados financieros auditados y preliminares trimestrales en formato PDF firmados digitalmente: hasta quince (15) días hábiles.

- Para la remisión de las informaciones de corte anual establecidas en la Resolución 01-2024: hasta diez (10) días hábiles.

- Para la remisión de las informaciones de corte mensual establecidas en la Resolución 01-2024: hasta cinco (5) días hábiles.

- Para la remisión de las informaciones de corte diario establecidas en la Resolución 01-2024: hasta tres (3) días hábiles, plazo en el cual deben estar al día todas las remisiones de los tres días posteriores a la remisión para la cual fue aprobada la prórroga.

5. Aprobación: La aprobación se comunicará por escrito y/o los medios digitales y estará firmada y sellada por la Superintendencia. Remisión de Información por Servicios Web (APIs)

Este canal permite una comunicación directa y automatiza entre los sistemas de la entidad y la Superintendencia, eliminando la entrada manual de datos, reduciendo errores y garantizando información actualizada en tiempo real.

Las APIs se basan en estándares abiertos (HTTP, JSON, XML), lo que facilita la integración con diversos sistemas (ERP, CRM, etc.). Para los detalles técnicos de los formatos de datos, consulte el, consulte el **Manual Para el Registro de Datos en Cumplimiento con la Resolución 01-2024**.

5.1 Configuración Inicial:

1. Autenticación:

   - Obtenga los tokens de acceso o API Keys proporcionados por la Superintendencia.

   - Asegúrese de incluir las cabeceras HTTP requeridas en cada solicitud (ej. Authorization, Content-Type).

2. Endpoints:

Obtenga acceso a los endpoints específicos (URL base, nombre del servicio, propósito y método HTTP).

Ejemplos de Endpoints:

Endpoint	**Propósito**	**Método**

/api/polizas_suscritas_personas	Información de Pólizas Suscritas	POST
/api/siniestros_reportados	Siniestros Reportados y su Estado	POST

3. Estructura de Solicitudes (Payload):

Para cada endpoint, estructure el cuerpo de la solicitud (payload) en el formato especificado (JSON/XML), incluyendo todos los campos requeridos y tipos de datos.

4. Manejo de Respuestas:

Prepare su sistema para manejar respuestas exitosas (ej. HTTP 200 OK, 201 Created) y de error (ej. HTTP 4xx, 5xx) según la documentación de la API.

5.2 Estructura de la Data:

Las informaciones remitidas vía servicios web, utilizan los mismos campos definidos en las plantillas de la oficina virtual. La descripción detallada de los campos y parámetros será suministrada por el área de tecnología de la Superintendencia.

5.3 Procedimientos a Considerar:

Las reglas sobre consistencia, estandarización, horarios de remisión, reenvío de información y solicitudes de prórroga descritas para la oficina virtual aplican de igual manera a este canal.

6. Remisión de información por FTP

El canal de remisión por Protocolo de Transferencia de Archivos (FTP) y sus variantes seguras (SFTP, FTPS) está disponible para la transferencia de archivos grandes o lotes de información de forma programada.

Este método es una alternativa efectiva para las instituciones que no disponen de sistemas que permitan la integración directa vía servicios web (APIs), o para la transferencia sencilla de archivos ya existentes, como informes en PDF o datasets en CSV. El uso de la aplicación FTP con interfaces gráficas facilita el envío manual de archivos a usuarios no técnicos.

Para conocer en detalle los formatos y la estructura de los datos a remitir, consulte el

Manual Para el Registro de Datos en Cumplimiento con la Resolución 01-2024.

A continuación, se detalla el proceso general para la remisión de información vía FTP.

6.1 Proceso de Remisión de Información por FTP

Paso 1: Obtener los datos de conexión

- Solicite y reciba de la Superintendencia la siguiente información:
    - Dirección del servidor FTP.
    - Puerto y protocolo a utilizar (FTP, SFTP o FTPS).
    - Nombre de usuario y contraseña asignados.

Paso 2: Preparar los archivos

- Asegúrese de que los archivos cumplan con los formatos (ej. CSV, TXT, XML, PDF) y las estructuras de datos especificadas por la Superintendencia.
- Nombre cada archivo siguiendo estrictamente las convenciones de nomenclatura establecidas, ya que es crucial para el procesamiento automático.

Paso 3: Disponer de un cliente FTP

- Instale y configure una aplicación FTP. La Superintendencia podría recomendar un software específico. Ejemplos de clientes son FileZilla, WinSCP, Cyberduck o herramientas de línea de comandos.

Paso 4: Establecer la conexión con el servidor

- Abra la aplicación FTP.
- Ingrese los datos de conexión: dirección del servidor, puerto, nombre de usuario y contraseña.
- Seleccione el protocolo correcto (FTP, SFTP, FTPS) según lo indicado.
- Inicie la conexión.

Paso 5: Navegar al directorio de carga

- Una vez conectado, navegue hasta la carpeta o directorio específico en el servidor designado para la carga de archivos. La Superintendencia debe proveer esta ruta.

Paso 6: Transferir los archivos

- En la aplicación FTP, seleccione los archivos preparados desde su equipo local.
- Utilice la función de "upload" (cargar o subir) para transferirlos al directorio designado en el servidor.
- Asegúrese de usar el modo de transferencia correcto (ej. Binario o ASCII) según el tipo de archivo y las especificaciones recibidas.

Paso 7: Verificar la carga

- Confirme en la aplicación FTP que la transferencia se completó totalmente y sin errores.
- Verifique que los archivos aparecen listados correctamente en el directorio del servidor.
- Siga cualquier procedimiento adicional de confirmación que la Superintendencia establezca (ej. enviar una notificación por correo electrónico).

Paso 8: Desconectar la sesión

- Al finalizar, cierre la conexión de forma segura utilizando la opción "desconectar" o "salir" de la aplicación FTP.

6.2. Procedimientos a considerar para la remisión

Las reglas sobre consistencia y estandarización de datos, horarios de remisión, reenvío de información y solicitudes de prórroga que aplican para la Oficina Virtual son igualmente válidas para este canal de remisión.

7. Remisión de información vía GRC

La remisión de información a través de un software de Gobernanza, Riesgo y Cumplimiento (GRC) es un proceso altamente estructurado, automatizado y seguro. Este método no es un simple envío de archivos, sino un flujo integral diseñado para consolidar y presentar datos críticos a las autoridades competentes. Para conocer en detalle los formatos de las plantillas o la estructura de los datos a remitir, consulte el ***Manual de Para el Registro de Datos en Cumplimiento con la Resolución 01-2024 Sobre Requerimientos y Remisión de Información y el anexo Sistema De Gobernanza, Riesgo Y Cumplimiento (GRC).***

A continuación, se detalla el proceso general para la remisión de información desde un entorno GRC:

7.1 Proceso de Remisión de Información por GRC

Paso 1: Preparar los Datos en el Software GRC

El software GRC funciona como un repositorio central para toda la información relevante.

La preparación de los datos incluye:

- **Recopilación y Consolidación:** Los datos necesarios para la remisión (pólizas, siniestros, estados financieros, etc.) residen en los módulos del software GRC. Estos pueden ser ingresados manualmente, importados o, idealmente, integrados de forma automática desde otros sistemas de la organización (ERP, CRM, sistemas contables).

- **Normalización y Estandarización:** El software GRC se encarga de que los datos cumplan con la estructura y los formatos predefinidos exigidos por la autoridad reguladora (ej. JSON, XML, CSV).

- **Validación Automática:** Antes de la remisión, la plataforma GRC ejecuta validaciones automáticas para verificar:

    - **Completitud:** Que todos los campos requeridos estén presentes.
    - **Formato:** Que los tipos de datos (fechas, números, texto) sean correctos.
    - **Integridad:** Que las referencias entre datos sean válidas (ej. un siniestro asociado a una póliza existente).
    - **Reglas de Negocio:** Que los valores cumplan con las reglas específicas de la resolución (ej. rangos de fechas, valores permitidos).
    - El sistema reportará cualquier error, impidiendo la remisión hasta que sea corregido.

Paso 2: Configurar la Remisión

El módulo de remisión del software GRC permite definir cómo y cuándo se enviará la información.

- **Definir Remisiones:** Configure un perfil para cada tipo de remisión requerida (ej. "Remisión Mensual de Pólizas"). Esto incluye:
    - **Frecuencia:** Diaria, semanal, mensual, trimestral o anual.
    - **Fechas de Corte:** El período que abarca la información.
    - **Endpoint de Destino:** La URL del Servicio Web (API) de la Superintendencia.
    - **Formatos de Salida:** JSON, XML, etc..

- **Programar la Ejecución:** Las remisiones pueden programarse para ejecutarse automáticamente en fechas y horas específicas, asegurando el cumplimiento de los plazos.

- **Gestionar Credenciales:** El software GRC gestiona de forma segura los tokens de acceso (Bearer tokens) o API Keys necesarios para autenticarse con la API de destino, incluyendo su obtención, renovación y rotación.

Paso 3: Ejecutar la Remisión vía Servicios Web (APIs)

Este paso cubre la conexión e interacción directa del software GRC con el sistema receptor.

- **Generar el Payload:** El sistema GRC construye el cuerpo de la solicitud (payload) en el formato (JSON o XML) requerido por la API de destino, basado en los datos ya validados.

- **Enviar la Solicitud HTTP:**
  - El software realiza una solicitud HTTP (POST o PUT) al endpoint especificado de la API.
  - Incluye las cabeceras HTTP necesarias, como Authorization: Bearer [token] y Content-Type: application/json.
  - El cuerpo de la solicitud contiene los datos a remitir.

- **Manejar las Respuestas de la API:** El software GRC interpreta la respuesta de la API de destino:

  - **Respuesta Exitosa (HTTP 200 OK, 201 Created):** Si la remisión es exitosa, el GRC registra el remission_id devuelto por la API para fines de trazabilidad y actualiza el estado a "Enviada" o "Procesada".

  - **Respuesta de Error (HTTP 4xx, 5xx):** Si la API devuelve un error (ej. 400 Bad Request, 401 Unauthorized), el software registra el error detalladamente, puede intentar reintentos automáticos si el error es temporal y genera alertas a los administradores si el problema requiere intervención.

Paso 4: Realizar Seguimiento y Trazabilidad

El software GRC proporciona una visibilidad completa del estado de todas las remisiones.

- **Utilizar el Dashboard:** Monitoree el tablero centralizado para ver el estado de cada remisión (programada, en proceso, exitosa, con errores).

- **Consultar el Historial:** Acceda a un registro completo de todas las remisiones, que incluye fecha, hora, estado, remission_id y logs detallados de la solicitud y respuesta.

- **Gestionar Alertas:** El sistema puede ser configurado para enviar notificaciones sobre fallos en la remisión, retrasos o confirmaciones de éxito.

7.2 Requisito para Empresas de Tercerización:

Las empresas de tercerización que actúen como emisores de información deben facilitar a la Superintendencia el acceso a su plataforma GRC, permitiendo la capacidad de consultar,

extraer, exportar y analizar la data en tiempo real.

8. Plataforma tecnológica requerida

8.1 Empresas aseguradoras y reaseguradoras

Para cumplir con las normativas de remisión de información digital y los requisitos de seguridad cibernética establecidos en las leyes y resoluciones de la República Dominicana, las empresas aseguradoras y reaseguradoras deben contar con una serie de capacidades tecnológicas mínimas. Estas capacidades mínimas requeridas, facilitan la capacidad de integración con la plataforma de servicios digitales de la Superintendencias.

Para conocer la descripción detallada de estas capacidades, consulte el anexo *Capacidad tecnológica requerida para empresas aseguradoras y reaseguradoras.*

8.2 Empresas de tercerización.

Se espera que las empresas de tercerización cumplan con los mismos requisitos mínimos que las aseguradoras y, adicionalmente, adopten tecnologías y prácticas más avanzadas para la gestión de la información y la seguridad. Estas expectativas se derivan de la complejidad administrativa y de seguridad que deben asumir como integradores de servicios.

Para conocer la descripción detallada de estas capacidades, consulte el anexo *Capacidad tecnológica requerida para empresas de tercerización.*

Adicionalmente, si las empresas de tercerización incluyen procesamiento de pagos en sus plataformas, es de rigor dar cumplimiento a las regulaciones y directrices establecidas por la RSCI para cumplir lo referente a "operaciones y servicios financieros asociados a los medios de pagos electrónicos", según se establece en el anexo *Pasarela de pagos.*

Dr. Julio César Valentín
Superintendente

Directora Jurídica | Encargado de Proyectos | Encargado de Tecnología

II. ANEXOS

ANEXO 1: CAPACIDAD TECNOLÓGICA REQUERIDA PARA EMPRESAS ASEGURADORAS Y REASEGURADORAS

Para cumplir con las normativas de remisión de información y los requisitos de ciberseguridad, las empresas aseguradoras y reaseguradoras deben contar con las siguientes capacidades tecnológicas mínimas:

1. Infraestructura Tecnológica y Hardware:

- **Sistemas y Equipos:** Poseer sistemas informáticos e infraestructura adecuados para procesar, almacenar y transmitir información de manera eficiente y segura (RSCI Art. 1, Art. 5 kk).
- **Almacenamiento:** Contar con sistemas de almacenamiento de red protegidos con controles de seguridad, que garanticen la confidencialidad, integridad y la disponibilidad de la información (RSCI Art. 26 c).
- **Conectividad:** Disponer de una conexión a Internet estable y segura para comunicarse con las plataformas de la Superintendencia (Oficina Virtual, FTP, APIs).
- **Resguardo de Información:** Realizar copias de respaldo de forma regular, incluyendo medios no conectados a la red interna. La información esencial debe ser cifrada y cumplir con los tiempos de retención definidos (RSCI Art. 26 e), i))
- **Continuidad del Negocio:** Definir procesos para garantizar la continuidad de las operaciones tecnológicas, incluyendo sistemas e infraestructuras flexibles, instalaciones alternativas o redundantes, y planes de recuperación ante desastres (RSCI Art. 40). Realizar pruebas de estrés anuales y simulacros de respuesta a incidentes (RSCI Art. 40 f)).

2. Software y Sistemas

- **Generación de Datos:** Disponer de sistemas capaces de generar y gestionar datos en los formatos especificados (PDF con firma digital, CSV, JSON, XML).
- **Herramientas de Remisión:**
    - Navegador web actualizado para usar la Oficina Virtual (SIRIS).
    - Software cliente FTP (ej. FileZilla) si se utiliza este canal.
    - Capacidad para interactuar con Servicios Web (APIs), incluyendo la gestión de tokens de acceso (API Keys).

- Opcionalmente, software GRC que pueda integrarse con los sistemas de la Superintendencia.

- **Actualizaciones:** Mantener un proceso para el despliegue de actualizaciones de seguridad en firmware, sistemas operativos y aplicaciones (RSCI Art. 30 a)).
- **Firma Digital:** Contar con herramientas para crear y usar firmas digitales que cumplan con la Ley 126-02 (unicidad, verificabilidad, control exclusivo y vinculación).

3. Conectividad y Red

- **Acceso Seguro:** Garantizar la conexión segura a los sistemas de la Superintendencia a través de los canales establecidos (HTTPS, FTP/SFTP, APIs).
- **Seguridad de Red:** Implementar y mantener firewalls con reglas de seguridad adecuadas (RSCI Art. 28 d)). Proteger los puntos de acceso a la red con mecanismos de control (RSCI Art. 28 b)).
- **Conexiones Externas:** Identificar, verificar, registrar y aprobar todas las conexiones de redes externas (RSCI Art. 28 c)).
- **Redes Inalámbricas:** Limitar el acceso a usuarios y dispositivos autorizados, y cifrar siempre el canal de transmisión (RSCI Art. 28 f)).

4. Gestión y Seguridad de la Información

- **Calidad de Datos:** Asegurar que los datos personales sean ciertos, adecuados, pertinentes, exactos y estén actualizados (Ley 172-13 Art. 5.2).
- **Programa de Ciberseguridad:** Establecer un programa formal que incluya políticas, procesos y estrategias para la seguridad (RSCI Art. 6, Art. 5 zz)).
- **Controles y Políticas:** Implementar gestión de activos, controles en aplicaciones de negocio, políticas de privacidad, soluciones criptográficas, autenticación robusta, protección contra malware, gestión de vulnerabilidades y monitoreo de eventos (RSCI Art. 19, 20, 21, 27, 30).
- **Protección de Datos Personales:** Cumplir con la Ley No. 172-13, adoptando todas las medidas técnicas y organizativas para proteger los datos personales (Ley 172-13 Art. 1, 5.5).

5. Personal y Procedimientos

- **Personal Capacitado:** Contar con personal competente para implementar y ejecutar el programa de ciberseguridad (RSCI Art. 10, 12 P.I).
- **Gestión de Cambios:** Aplicar un proceso definido para la gestión de cambios en sistemas e infraestructura para no afectar los servicios (RSCI Art. 26 d)).
- **Autoevaluación:** Realizar autoevaluaciones periódicas para verificar el cumplimiento (RSCI Art. 46).

6. Servicios de Terceros

- **Contratación:** Si se utilizan terceros para la remisión de información, estos deben cumplir con los requisitos regulatorios y tecnológicos establecidos por la Superintendencia.
- **Gestión de Proveedores:** Establecer un proceso formal para la selección y gestión de proveedores externos, con acuerdos que especifiquen los requisitos de ciberseguridad (RSCI Art. 36 a)).

ANEXO 2: CAPACIDAD TECNOLÓGICA REQUERIDA PARA EMPRESAS DE TERCERIZACIÓN

Las empresas de tercerización deben cumplir con los requisitos mínimos establecidos para las aseguradoras y, adicionalmente, adoptar prácticas y tecnologías más avanzadas dada la complejidad y responsabilidad que asumen como integradores de servicios.

A continuación, se detallan estos requisitos avanzados:

1. Canales de Remisión y Automatización Avanzada:

- **Uso Preferente de Servicios Web (APIs):** Utilizar preferentemente los Servicios Web (APIs), microservicios o servicios en la nube para una remisión de información automatizada, programática, continua y en tiempo real. Esto minimiza la entrada manual de datos y reduce los errores.
- **Capacidad Técnica para APIs:** Demostrar la capacidad para gestionar la configuración técnica de las APIs, incluyendo la autenticación mediante tokens de acceso (API Keys), el manejo de cabeceras HTTP y la correcta estructuración de las solicitudes (payloads) en JSON o XML.
- **Implementación de Plataformas GRC:** Utilizar una herramienta de Gobernanza, Riesgo y Cumplimiento (GRC) para la remisión de información. Se contempla que la remisión se realice mediante plataformas GRC, descritas como un proceso "altamente estructurado, automatizado y seguro". Esto implica usar el software GRC como un "repositorio central" con capacidad de integración automática y programación de remisiones

2. Integración de Sistemas y Automatización de Procesos:

- **Comunicación Directa y Programática:** Automatizar el flujo de información desde sus sistemas internos hasta la Superintendencia, eliminando la dependencia de ciclos de remisión manual.
- **Integración con Sistemas Centrales (Core):** Facilitar la integración de los sistemas de remisión con sistemas internos como ERP, CRM y sistemas contables para un ecosistema digital cohesivo y una visión 360° de la información.

3. Seguridad Cibernética Sofisticada y Robusta: Las empresas de tercerización deben demostrar una implementación más profunda de la seguridad, acorde a su "naturaleza, tamaño, complejidad, perfil de riesgo e importancia sistémica", implementando herramientas avanzadas. (Ver anexo: Herramientas Avanzadas para la Seguridad Cibernética).

- **Monitoreo Continúo Avanzado:** Implementar herramientas y procesos avanzados para el monitoreo continuo de los controles de seguridad de los sistemas y la infraestructura.

- **Gestión de Identidad y Acceso Fortalecidos:** Utilizar mecanismos robustos para la gestión de identidad, autenticación y control de acceso, incluyendo auditorías periódicas de los permisos otorgados.
- **Gestión Proactiva de Vulnerabilidades:** Establecer un proceso avanzado para el análisis, monitoreo y evaluación de vulnerabilidades, empleando soluciones de prevención y detección de intrusos.
- **Desarrollo Seguro de Aplicaciones:** Si desarrollan software, deben seguir una metodología de desarrollo seguro documentada, con entornos separados de prueba y producción, y realizar pruebas de seguridad exhaustivas (pruebas de penetración, control de acceso) antes del despliegue.
- **Adhesión a Estándares Internacionales:** Estar en capacidad de implementar y certificar el cumplimiento de normas internacionales relevantes como PCI-DSS, PA-DSS, SWIFT-CSCF, entre otras, cuando aplique.

4. Gobernanza de Datos y Calidad Superior:

- **Marcos de Gobernanza Formales:** Implementar marcos de gobernanza de datos bien definidos y robustos para asegurar la calidad, integridad, confidencialidad y el ciclo de vida de la información.
- **Validación y Normalización Automatizada:** Utilizar capacidades avanzadas y automatizadas para la validación de la información y la normalización de datos antes de la remisión, como las descritas para sistemas GRC. Esto se alinea con el principio de calidad de los datos de la Ley 172-13.
- **Gestión Sistemática de Activos:** Mantener un esquema de gestión de activos de información que incluya clasificación, gestión de documentos estructurada y un repositorio actualizado de sistemas y equipos tecnológicos.

5. Resiliencia Operativa y Continuidad del Negocio Mejoradas:

- **Infraestructura Flexible y Robusta:** Disponer de sistemas e infraestructuras tecnológicas más flexibles, con equipos y sistemas robustos y confiables.
- **Instalaciones Alternativas y Redundantes:** Implementar instalaciones alternativas o redundantes para los sistemas críticos.
- **Planes de Recuperación y Pruebas Rigurosas:** Mantener planes de recuperación ante desastres bien documentados y probados regularmente, con pruebas de estrés que pueden ser más frecuentes o complejas según el perfil de riesgo.

6. Soporte y Mantenimiento:

Nivel 1 (L1) - Soporte Básico: Punto de contacto inicial para resolver problemas comunes como consultas frecuentes o restablecimiento de contraseñas. Su objetivo es resolver la mayor cantidad de incidentes en el primer contacto.

Nivel 2 (L2) - Soporte Técnico Especializado: Maneja incidentes que requieren un conocimiento técnico más profundo de la plataforma y sus integraciones. Realiza diagnósticos avanzados y análisis de logs.

Nivel 3 (L3) - Soporte de Desarrollo o Infraestructura: Nivel más especializado, encargado de problemas complejos relacionados con fallos en el código, la arquitectura o la infraestructura subyacente. Desarrolla soluciones permanentes como parches o nuevas versiones.

7. Canales de Soporte:

- **Correo Electrónico:** Para la comunicación formal, documentación de incidentes y seguimiento de casos no urgentes.
- **Teléfono:** Crucial para la atención de incidentes críticos que requieren una respuesta inmediata.
- **Portal de Gestión de Tickets (CRM/Service Desk):** Plataforma web para que los usuarios creen y gestionen sus tickets de soporte de forma autogestionada. Centraliza todas las interacciones, asigna prioridades y asegura la trazabilidad de cada caso.
- **Chat de Soporte (en línea):** Para ofrecer asistencia en tiempo real para consultas rápidas y problemas menores.

8. Capacitación y documentación.

Capacitación:

- Presentar un plan de capacitación anual para guiar a los usuarios en el uso efectivo de la plataforma.
- Ofrecer distintas modalidades (presencial, semipresencial o virtual).
- Utilizar diversos métodos como tutoriales, videos, ejemplos prácticos y sesiones de preguntas y respuestas.

Documentación:

- Entregar un manual de usuario con instrucciones paso a paso, consejos de solución de problemas e información de seguridad.
- Entregar un manual de administrador con información detallada sobre la configuración, gestión del sistema y seguridad.

9. Base de conocimiento.

- Facilitar una base de conocimiento con contenido estructurado y accesible para la resolución de dudas y la consulta de mejores prácticas.
- Se recomienda el uso de software especializado, plataformas wiki o chatbots para su implementación.

ANEXO 3: HERRAMIENTAS AVANZADAS PARA LA SEGURIDAD CIBERNÉTICA

Aunque las normativas no enumeran marcas específicas, sí describen funcionalidades que implican el uso de categorías avanzadas de herramientas de ciberseguridad, especialmente para entidades con mayor madurez tecnológica como las empresas de tercerización. A continuación, se describen estas herramientas y capacidades avanzadas.

1. Herramientas de Detección, Respuesta y Análisis de Amenazas:

- **Sistemas de Detección/Prevención de Intrusos de Próxima Generación (NG-IPS/IDS) y Firewalls de Próxima Generación (NGFW):**
    - Función: Ofrecen capacidades avanzadas como inspección profunda de paquetes, conocimiento de aplicaciones y prevención de amenazas conocidas y desconocidas.

- **Base Normativa y Aplicación:**
    - El Reglamento de Seguridad Cibernética y de la Información (RSCI) exige el uso de firewalls con reglas de seguridad para el tráfico de datos (RSCI Art. 28 d)).
    - El RSCI también requiere la implementación de soluciones o mecanismos de prevención y detección de intrusos (RSCI Art. 30 e)).
    - El Instructivo SIRIS menciona la necesidad de firewalls para la seguridad de los canales de remisión.

- **Endpoint Detection and Response (EDR) y Extended Detection and Response (XDR):**
    - Función: Proporcionan monitoreo continuo y respuesta avanzada en los puntos finales (endpoints) y a través de múltiples capas de seguridad. Van más allá de la protección antimalware básica requerida por el RSCI (Art. 30 b)).

- **Security Information and Event Management (SIEM) Avanzado:**
    - Función: No solo centralizan el "registro de eventos de seguridad" (RSCI Art. 30 c)), sino que utilizan análisis avanzados, inteligencia artificial y correlación para detectar incidentes complejos y facilitar la respuesta.

- **Network Detection and Response (NDR):**
    - Función: Para un "monitoreo de los sistemas y la infraestructura tecnológica" más profundo (RSCI Art. 30 d)), estas herramientas analizan el tráfico de red para detectar actividades maliciosas que otras soluciones podrían pasar por alto.
- **Plataformas de Inteligencia de Amenazas (TIPs):**
    - Función: Enriquecen los sistemas de seguridad con información contextualizada sobre amenazas nuevas y emergentes, lo que ayuda a gestionar las "vulnerabilidades y amenazas tecnológicas" (RSCI Art. 30).

2. Herramientas Avanzadas para la Seguridad de Datos:

- **Soluciones de Prevención de Fuga de Información (Data Loss Prevention - DLP)**
    - **Función:** Implementan mecanismos robustos para la "protección contra la fuga de información" en sistemas, infraestructura y entornos locales que procesan, almacenan o transmiten información sensible (RSCI Art. 27 e)).
- **Criptografía Avanzada y Gestión de Claves**
    - **Función:** Se deben usar "soluciones criptográficas para proteger y preservar la confidencialidad e integridad de la información sensible en tránsito o almacenada" (RSCI Art. 27 d)). Esto incluye el uso de algoritmos robustos y una "gestión segura de las llaves criptográficas" (RSCI Art. 27 d) i), ii)), posiblemente con el apoyo de Módulos de Seguridad de Hardware (HSM).

3. Herramientas para la Gestión de la Seguridad y Operaciones

- **Herramientas de Evaluación de Vulnerabilidades y Pruebas de Penetración (VAPT)**
    - **Función:** Son necesarias para cumplir con la ejecución de "pruebas de Seguridad Cibernética y de la Información... utilizando herramientas para la detección de vulnerabilidades, pruebas de penetración y pruebas de control de acceso" (RSCI Art. 38 e)).
- **Plataformas de Gobernanza, Riesgo y Cumplimiento (GRC)**
    - **Función:** El Instructivo SIRIS las describe como un medio avanzado para la remisión de información, que incluye consolidación de datos, validación automática, integración vía API y seguimiento detallado (Instructivo SIRIS Sección 7).

- **Herramientas de Orquestación, Automatización y Respuesta (SOAR)**
    - **Función:** Permiten automatizar y agilizar la respuesta a incidentes de seguridad, complementando la "gestión de incidentes de seguridad cibernética y de la información" (RSCI Art. 31).
- **Herramientas de Investigación Forense Digital**
    - **Función:** Son requeridas para realizar "investigaciones forenses relacionadas a incidentes de seguridad cibernética y de la información" (RSCI Art. 31 c)).

4. Adopción de Estándares Internacionales:

- **Función:** Las empresas tecnológicamente maduras deben tener la capacidad de implementar las tecnologías y procesos necesarios para alinearse con marcos internacionales.
- **Base Normativa y Aplicación:** El RSCI (Art. 44 y 45) requiere el cumplimiento de objetivos de varios estándares como PCI-DSS, PCI-PTS, PA-DSS, SWIFT-CSCF, PCI P2PE y PCI-TSP, cuando aplique.

ANEXO 4: SISTEMA DE GOBERNANZA, RIESGO Y CUMPLIMIENTO (GRC)

Un sistema GRC es una plataforma de software diseñada para ayudar a las organizaciones a gestionar de forma integrada la gobernanza, los riesgos y el cumplimiento normativo. En el contexto de la remisión de información, un software GRC facilita un proceso estructurado, automatizado y seguro.

1. Características Principales de un Sistema GRC

- Repositorio Centralizado: Actúa como un punto único para toda la información relevante (pólizas, siniestros, etc.), la cual puede ser integrada automáticamente desde otros sistemas como ERP o CRM.
- Normalización y Estandarización: Asegura que todos los datos cumplan con los formatos y estructuras exigidos por la autoridad reguladora (ej. JSON, XML).
- Validación Automática: Antes de la remisión, ejecuta validaciones para verificar la completitud, formato, integridad y cumplimiento de reglas de negocio, reportando errores para su corrección.
- Configuración y Programación de Remisiones: Permite definir y programar la ejecución automática de las remisiones (frecuencia, fechas de corte, etc.), asegurando el cumplimiento de plazos.
- Envío Seguro y Automatizado: Construye el cuerpo de la solicitud (payload) y lo envía de forma segura al API de la Superintendencia, gestionando la autenticación (ej. Bearer tokens).
- Manejo Inteligente de Respuestas: Interpreta las respuestas del API, registrando confirmaciones de éxito o gestionando errores, con capacidad de reintentos automáticos y generación de alertas.
- Seguimiento y Trazabilidad: Ofrece un dashboard para visualizar el estado de todas las remisiones y mantiene un historial detallado que sirve como pista de auditoría.
- Capacidades Analíticas: Permite usar los datos para generar inteligencia de negocio, analizar riesgos e identificar patrones de incumplimiento.

2. Gestión de Auditorías y Cumplimiento

Un sistema GRC es fundamental para la gestión de auditorías, ya que facilita la supervisión en tiempo real por parte de la Superintendencia y asegura el cumplimiento normativo mediante la automatización de controles y la generación de pistas de auditoría detalladas.

- Visión Predictiva del Cumplimiento: Sus capacidades analíticas y estadísticas proporcionan una visión profunda y predictiva sobre el estado del cumplimiento de la organización.

- Facilitador de la Supervisión: Permite a la Superintendencia tener la capacidad de consultar, extraer, exportar y analizar la data en tiempo real sobre la misma plataforma, agilizando la supervisión y la provisión de servicios controlados.
- Aseguramiento del Cumplimiento Normativo**:** Todo el proceso está diseñado para minimizar errores y asegurar el cumplimiento normativo en la remisión de información.
- Pista de Auditoría Detallada: El historial completo y los logs detallados de las remisiones sirven como una pista de auditoría esencial para revisiones internas y externas.
- Automatización de Controles: El GRC puede automatizar la verificación del cumplimiento de las reglas de la resolución antes del envío.

3. Esquemas de Seguridad Cibernética

El software GRC opera dentro de un marco de ciberseguridad robusto y lo refuerza mediante:

- Proceso Seguro de Remisión: El envío de información es descrito como un proceso inherentemente seguro y automatizado.
- Gestión Segura de Credenciales: Gestiona de forma segura los tokens de acceso y API Keys necesarios para la autenticación.
- Alineación con Políticas: Debe operar en consonancia con las políticas de ciberseguridad (RSCI) y protección de datos (Ley 172-13) de la entidad..

ANEXO 5: FIRMA DIGITAL

Uso de la Firma Digital para la Remisión de Documentos (Según Ley No. 126-02, RD)

La Ley No. 126-02 de la República Dominicana es el marco que reconoce la validez jurídica y fuerza probatoria de la firma digital, otorgándole los mismos efectos que una firma manuscrita.

1. **Principios Clave de la Ley 126-02**

Para que una firma digital sea válida, debe cumplir con los siguientes atributos:

- **Unicidad:** Ser única a la persona que la usa.
- **Verificabilidad:** Ser susceptible de ser verificada.
- **Control Exclusivo:** Estar bajo el control exclusivo del firmante (su clave privada).
- **Vinculación:** Estar ligada a la información de tal manera que cualquier cambio posterior invalide la firma, garantizando la integridad del documento.
- **Conformidad Regulatoria:** Cumplir con las reglamentaciones adoptadas por el Poder Ejecutivo.

2. **Proceso de Uso de la Firma Digital para la Remisión**

- **Paso 1: Obtención de un Certificado Digital**
    - La entidad debe adquirir un certificado digital de una Entidad de Certificación autorizada por el INDOTEL. Este certificado asocia la identidad del firmante a su clave pública.
- **Paso 2: Aplicación de la Firma Digital**
    - El sistema del remitente calcula un valor
    - hash (resumen criptográfico) del documento digital.
    - Este hash se cifra utilizando la clave privada del firmante. El resultado de esta operación es la firma digital.
    - La firma digital se adhiere al documento (ej. incrustada en un PDF) y se remite junto con el certificado digital.
- **Paso 3: Verificación por Parte del Receptor**

- El sistema de la Superintendencia utiliza la clave pública del firmante (obtenida del certificado) para descifrar la firma y recuperar el hash original.
- Paralelamente, calcula un nuevo hash del documento recibido.
- Si ambos hashes coinciden, se confirma que el documento es auténtico (proviene del firmante), íntegro (no ha sido alterado) y cumple con el principio de no repudio (el firmante no puede negar haberlo enviado).

ANEXO 6: REGLAMENTO DE LA SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN (RSCI)

14 de mayo 2018

Este Reglamento tiene por objeto establecer los principios y lineamientos generales que servirán de base a las entidades de intermediación financiera, los administradores y participantes del Sistema de Pagos y Liquidación de Valores de la República Dominicana (SIPARD) y, de los sistemas de pago y liquidación de valores que lo componen; y, a las entidades de apoyo y servicios conexos interconectadas con las entidades de intermediación financiera y con el SIPARD, para procurar la integridad, disponibilidad y confidencialidad de la información, el funcionamiento óptimo de los sistemas de información y de la infraestructura tecnológica, así como la adopción e implementación de prácticas para la gestión de riesgos de la Seguridad Cibernética y de la Información, acorde a su naturaleza, tamaño, complejidad, perfil de riesgo e importancia sistémica, conforme a la Ley No.183-02, Monetaria y Financiera de fecha 21 de noviembre del 2002 y sus modificaciones, y a los estándares internacionales en la materia.

A continuación, presentamos los artículos de mayor relevancia que serán aplicables a los procesos de consulta, remisión e integración de la información requerida por la Superintendencia de Seguros.

Articulo 19. Gestión de Activos de Información. Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas mixtas de intermediación financiera y, las entidades de apoyo y servicios conexos deben desarrollar un esquema de gestión de activos de información que contemple los aspectos siguientes:

a) Clasificación de Activos de Información: La clasificación de los activos de información se llevará a cabo de acuerdo con el nivel de confidencialidad de la Información y el nivel de sensibilidad de la información que gestionan;

b) Gestión de Documentos: Los documentos deben ser manejados de una manera sistemática y estructurada, debiéndose cumplir con los requisitos de Seguridad Cibernética y de la Información a lo largo del ciclo de vida del documento;

c) Información Sensible en Formato Físico: La información sensible en formato físico, debe protegerse contra la corrupción, la pérdida o la divulgación no autorizada; y,

d) Registro de Activos de Información: Los sistemas informáticos y equipos de la infraestructura tecnológica, deben ser registrados en un repositorio, el cual deberá permanecer actualizado.

Artículo 20. Aplicaciones del Negocio. Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas mixtas de intermediación financiera y, las entidades de apoyo y servicios conexos, implementarán controles de

seguridad para las aplicaciones del negocio que contemplen los aspectos siguientes:

a) Protección de las Aplicaciones: Las aplicaciones de negocios deben utilizar funcionalidades de seguridad de la información alineadas a la infraestructura técnica de seguridad, que permitan el cumplimiento de los requerimientos de confidencialidad, integridad y disponibilidad de la información;

b) Protección de las Aplicaciones Basadas en Navegación: Se deben establecer controles específicos de seguridad cibernética sobre las aplicaciones internas que apoyan los servicios hacia Internet, basadas en el navegador y en los servidores en donde se ejecutan; y,

c) Validación de la Información: Las aplicaciones del negocio deben incorporar controles de Seguridad Cibernética y de la Información, que protejan la confidencialidad e integridad de la información, cuando sean ingresadas, procesadas o extraídas de la aplicación.

Artículo 21. Políticas de Privacidad de la Información. Las entidades de intermediación financiera, los administradores y participantes del SIP ARD, las entidades públicas mixtas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben establecer y dar a conocer en los contratos y en cualquier otro medio electrónico de comunicación con sus clientes, las políticas relacionadas a la privacidad de la información y datos de carácter personal utilizados en sus productos y servicios, así como cualquier modificación a las mismas. Estas políticas deberán contener el desglose del uso que la entidad receptora de Información dará a cada tipo de información o dato recopilado.

Artículo 28. Gestión de la Red. Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas mixtas de intermediación financiera y, las entidades de apoyo y servicios conexos, implementarán procesos y plataformas para la gestión segura de los componentes en las redes de información, tomando en consideración los aspectos siguientes:

a) Configuración de Dispositivos de Red: Los dispositivos de red deben ser configurados para funcionar de acuerdo con su rol y se establecerán controles de seguridad que eviten cambios no autorizados o incorrectos;

b) Gestión de la Red Física: Las redes deben ser protegidas por controles físicos de seguridad, con el apoyo de documentación actualizada y el etiquetado de los componentes esenciales. Los puntos de acceso a la red deben estar protegidos por mecanismos de control de acceso;

c) Conexiones de Redes Externas: Las conexiones de redes externas a los sistemas y redes informáticas deben ser identificadas, verificadas, registradas y aprobadas individualmente por el comité funcional de seguridad cibernética;

d) Tráfico de Datos a Través de los Firewalls (Cortafuegos): El tráfico de datos entre redes o subredes internas o externas interconectadas, será debidamente transmitido a través de firewalls, con las reglas de seguridad requeridas, previo a la concesión o restricción de acceso;

e) Mantenimiento Remoto: El mantenimiento remoto de los sistemas y redes críticas deberá restringirse al personal debidamente autorizado, confinado a sesiones individuales y sujeto a revisión;

Artículo 36. Gestión de Proveedores Externos de Productos o Servicios Tecnológicos. Las entidades de intermediación financiera, los administradores y participantes del SIP ARD, las entidades públicas mixtas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben asegurar las comunicaciones electrónicas de la organización, mediante controles y políticas de Seguridad Cibernética y de la Información, tomando en consideración los aspectos siguientes:

a) Tercerización: Se debe establecer un proceso para regir la selección y gestión de los proveedores externos, apoyado en acuerdos documentados que especifiquen los requisitos de Seguridad Cibernética y de la Información;

b) Requisitos de Seguridad a los Proveedores Externos: El cumplimiento de los requisitos de Seguridad Cibernética y de la Información, deben considerarse y revisarse de manera periódica a lo largo de la relación con los proveedores externos;

c) Adquisición o Arrendamiento de Equipos y Sistemas Tecnológicos: El proceso de adquisición o arrendamiento de equipos y sistemas tecnológicos, deberá prever requerimientos técnicos de seguridad aprobados por el comité funcional de Seguridad Cibernética y de la Información, asegurando que estos brinden la funcionalidad requerida y no comprometan la seguridad de la información sensible de la entidad; y,

d) Contratación de Servicios de Computación en la Nube: Se debe documentar una política para el uso y contratación de servicios de computación en la nube, que contemple el desarrollo de un análisis de riesgos de Seguridad Cibernética y de la Información de los servicios contratados, para determinar el uso de los mismos por parte de los colaboradores, la integridad de la información almacenada, así como los mecanismos de protección de la misma. Esta política debe ser comunicada a todos los colaboradores que puedan hacer uso de los mismos y los requerimientos de seguridad cibernética deben estar contenidos en dicha política.

Artículo 41. Auditorías Internas. Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas mixtas de intermediación financiera y, las entidades de apoyo y servicios conexos, establecerán procesos de auditorías internas para garantizar la supervisión efectiva el Programa de Seguridad Cibernética y de la Información, contemplando los aspectos siguientes:

a) Gestión de las Auditorías Internas de Seguridad Cibernética y de la Información: El estado de Seguridad Cibernética y de la Información en los sistemas de la información y la infraestructura tecnológica, debe ser objeto de auditorías exhaustivas y periódicas, llevadas a cabo por la unidad interna de auditoría o a través de una firma de auditores externos registrada en la Superintendencia de Bancos, en cumplimiento con el proceso de auditoría interna de la entidad; y,

b) Informes de Resultados de las Auditorías Internas de Seguridad Cibernética y de la

Información: Los resultados de las auditorías internas de Seguridad Cibernética y de la Información de los sistemas informáticos y la infraestructura tecnológica, deberán contener la documentación y notificación a las partes interesadas de sus conclusiones y recomendaciones.

Artículo 44. Estándares Internacionales. Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas mixtas de intermediación financiera y, las entidades de apoyo y servicios conexos, que de manera contractual accedan a los servicios prestados por entidades internacionales que habilitan la provisión de sus productos y servicios dentro de dicho sistema, deben cumplir, en cada caso en que aplique, con los objetivos siguientes:

a) Proteger los datos del cliente y facilitar la adopción de medidas de seguridad uniformes, apoyados en la Norma de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI-DSS, por sus siglas en inglés);

b) Asegurar la protección en la administración, procesamiento y transmisión, tanto en línea como fuera de línea, del Número de Identificación Personal (PIN, por sus siglas en inglés) del cliente, apoyados en los requerimientos de seguridad del PIN del grupo de estándares PCI - PTS;

c) Aplicar los requerimientos de seguridad y los procedimientos de evaluación de los proveedores de sistemas de aplicaciones de pago, apoyados en la Norma de Seguridad para las Aplicaciones de Pago (PA-DSS, por sus siglas en inglés); y,

d) Reforzar los controles de seguridad de los ambientes locales e infraestructuras relacionadas que interactúen con la red de SWIFT, apoyado en el Marco de Controles de Seguridad del Cliente (SWIFT - CSCF, por sus siglas en inglés).

ANEXO 7: POLITICAS DE PROTECCIÓN DE DATOS

La Ley No. 172-13 sobre Protección Integral de Datos Personales es fundamental para la remisión de información, pues su objeto es garantizar los derechos fundamentales al honor, la intimidad y la autodeterminación informativa. El instructivo debe reflejar el cumplimiento de sus principios y obligaciones.

A continuación, se detallan las políticas de seguridad clave basadas en esta ley:

1. **Principio de Licitud y Finalidad**

(Art. 5, Num. 1 y 3)

- **Política:** La remisión de datos personales solo se realizará con una base legal clara (consentimiento, obligación legal, etc.) y para la finalidad específica para la cual fueron recolectados.
- **Implementación:**
    - El instructivo debe declarar la finalidad de cada remisión.
    - Asegurar que solo se remitan los datos estrictamente necesarios (minimización de datos).

2. **Principio de Calidad de los Datos**

(Art. 5, Num. 2)

- **Política:** Los datos remitidos deben ser adecuados, pertinentes, veraces, exactos y estar actualizados.
- **Implementación:**
    - Implementar validaciones robustas en los sistemas para garantizar la exactitud de los datos antes de la remisión.
    - Establecer procedimientos claros para la rectificación, actualización o cancelación de datos inexactos.

3. **Principio de Seguridad de los Datos**

(Art. 5, Num. 5; Art. 21)

- **Política:** Se deben implementar todas las medidas de seguridad técnicas, organizativas y físicas necesarias para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.
-
- **Implementación:**

- **Cifrado en Tránsito:** Exigir que todas las comunicaciones con los Servicios Web se realicen a través de HTTPS con una versión robusta de TLS.
- **Autenticación Fuerte:** Mantener el uso de protocolos seguros como OAuth 2.0 y gestionar los tokens de acceso de forma segura. Considerar MFA si aplica.
- **Firma Digital (Ley 126-02):** Reafirmar su uso para garantizar la integridad, autenticidad y no repudio de los documentos.
- **Monitoreo y Auditoría:** Registrar de forma exhaustiva todas las solicitudes y respuestas del API y monitorearlas activamente para detectar actividades sospechosas.
- **Protección contra Ataques:** Implementar medidas contra vulnerabilidades comunes (OWASP Top 10).

4. Principio de Confidencialidad y Secreto Profesional

(Art. 5, Num. 6; Art. 24)

- **Política:** Todo el personal que intervenga en el tratamiento de datos personales está obligado a guardar secreto profesional, incluso después de cesar sus funciones.
- **Implementación:**
  - Exigir acuerdos de confidencialidad (NDAs) al personal involucrado.
  - Proveer capacitación regular sobre la Ley 172-13 y la importancia de la protección de datos.

5. Gestión de Incidentes de Seguridad y Respuesta (Art. 21):

- **Política:** Se establecerán procedimientos claros para la **detección, gestión y notificación de incidentes de seguridad** que puedan afectar los datos personales remitidos o almacenados.

- **Implementación en el Instructivo:**

  - **Notificación:** Definir cómo y cuándo se notificará a las autoridades reguladoras y a los titulares de los datos (si aplica y si el incidente implica un riesgo para sus derechos) en caso de una brecha de seguridad que afecte la remisión.

  - **Plan de Contingencia:** El software GRC debe ser parte de un plan de continuidad de negocio y recuperación ante desastres que asegure la disponibilidad de los datos y la capacidad de remisión.

6. Derechos de los Titulares de Datos (Art. 10 y ss.):

- **Política:** Aunque la remisión es a una autoridad, la organización debe asegurar que la data remitida cumple con los derechos de acceso, rectificación, cancelación y oposición (ARCO) de los titulares de datos, cuando corresponda.

- **Implementación en el Instructivo:**
    - **Mecanismos ARCO:** Asegurar que el sistema fuente y el software GRC tengan mecanismos para procesar solicitudes ARCO antes de la remisión, para que los datos enviados sean correctos y reflejen las solicitudes del titular.

7. Transferencia Internacional de Datos (Art. 25):

- **Política:** Si el servidor de la API de destino o el almacenamiento de datos del receptor se encuentran fuera de la República Dominicana, la remisión solo se realizará si se cumplen las condiciones de la Ley 172-13 (ej., consentimiento del titular, país con nivel de protección adecuado).
- **Implementación en el Instructivo:**
    - **Ubicación de Servidores:** Indicar claramente la ubicación geográfica de los servidores donde se reciben y procesan los datos remitidos. Si es internacional, documentar el cumplimiento de la Ley 172-13 para dichas transferencias.

ANEXO 8: PASARELA DE PAGOS

Para operar en la República Dominicana, una pasarela de pagos en línea debe cumplir con rigurosos requisitos técnicos enfocados en la seguridad, la integridad de las transacciones y la protección de los datos. Estos requisitos se derivan principalmente del Reglamento de Seguridad Cibernética y de la Información (RSCI), la Ley de Protección de Datos Personales y el marco legal del comercio electrónico.

1. Cumplimiento de Estándares Internacionales de Seguridad

La adhesión a estándares internacionales es un requisito explícito, especialmente para el manejo de datos de tarjetas de pago:

- **PCI-DSS (Payment Card Industry Data Security Standard):** Es fundamental "proteger los datos del cliente y facilitar la adopción de medidas de seguridad uniformes, apoyados en la Norma de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI-DSS...)". Este estándar abarca requisitos para:
    - Construir y mantener una red y sistemas seguros.
    - Proteger los datos del titular de la tarjeta.
    - Mantener un programa de gestión de vulnerabilidades.
    - Implementar medidas sólidas de control de acceso.
    - Monitorear y probar regularmente las redes.
    - Mantener una política de seguridad de la información.
- **PA-DSS (Payment Application Data Security Standard):** Se deben "aplicar los requerimientos de seguridad y los procedimientos de evaluación de los proveedores de sistemas de aplicaciones de pago, apoyados en la Norma de Seguridad para las Aplicaciones de Pago (PA-DSS...)", si la pasarela utiliza o consiste en dicho software.
- **Cifrado Punto a Punto (P2PE):** Para "fortalecer la protección de los datos transmitidos desde el Punto de Interacción hasta su destino final, apoyados en los requerimientos de soluciones para el cifrado punto a punto (P2PE) del estándar PCI - P2PE".
- **Tokenización (PCI-TSP):** Es necesario "robustecer los controles de seguridad para salvaguardar la integridad del entorno de datos del Token, tanto estáticos como dinámicos, apoyados en los estándares de seguridad para proveedores de servicios de Token (PCI - TSP)", si se utiliza tokenización.

2. Seguridad de Sistemas de Información y Aplicaciones

La pasarela de pagos debe asegurar la "confiabilidad técnica", garantizando la disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento de sus sistemas.

- **Protección de Aplicaciones del Negocio (Pasarela):**
    - Debe utilizar "funcionalidades de seguridad de la información alineadas a la infraestructura técnica de seguridad" para cumplir con los requerimientos de confidencialidad, integridad y disponibilidad.
    - Establecer "controles específicos de seguridad cibernética sobre las aplicaciones internas que apoyan los servicios hacia Internet".
    - Incorporar controles que "protejan la confidencialidad e integridad de la información, cuando sean ingresadas, procesadas o extraídas de la aplicación".
- **Criptografía:** Se deben "utilizar soluciones criptográficas para proteger y preservar la confidencialidad e integridad de la información sensible en tránsito o almacenada", como los datos de pago.
- **Protección Contra Fuga de Información (DLP):** Se deben "establecerán mecanismos de protección contra la fuga de información a los sistemas, infraestructura tecnológica y entornos locales que procesan, almacenan o transmiten información sensible".
- **Gestión de Vulnerabilidades y Amenazas:** Se debe establecer un proceso para el "despliegue recurrente de actualizaciones de seguridad del firmware, de los sistemas operativos y de las aplicaciones", implementar "protección contra el software malicioso", asegurar el "registro de eventos de seguridad cibernética y de la información" con análisis regular, realizar el "monitoreo de los sistemas y la infraestructura tecnológica" y contar con "prevención y detección de intrusos".
- **Controles de Acceso:** Implementar procesos de concesión o denegación de solicitudes para obtener y utilizar información y servicios de procesamiento, o entrar en instalaciones físicas.

3. Protección de Datos Personales

Toda información personal manejada por la pasarela está sujeta a la Ley No. 172-13:

- **Medidas de Seguridad:** El responsable del tratamiento debe "adoptar e implementar las medidas de índole técnica, organizativa y de seguridad necesarias para salvaguardar los datos de carácter personal y eviten su alteración, pérdida, tratamiento, consulta o acceso no autorizado".
- **Deber de Secreto:** Quienes intervengan en el tratamiento de datos personales están

"obligados al secreto profesional respecto de los mismos y al deber de guardarlos".

4. Requisitos Operacionales y de Infraestructura

- **Disponibilidad y Continuidad del Negocio:** Se deben definir procesos para "garantizar la continuidad de las operaciones tecnológicas ante incidentes de Seguridad Cibernética y de la Información", incluyendo esquemas de continuidad, resiliencia y planes de recuperación ante desastres.

- **Integridad de Transacciones:** Asegurar que el "sistema de información" (la pasarela) procese las transacciones sin alteraciones no autorizadas y de manera confiable.

- **Autenticación:** Implementar un "acto de asegurar la identidad de un usuario para tener acceso a la información computarizada".

- **Registro y Pistas de Auditoría:** Mantener un "registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el propósito de mantener información histórica para fines de control, supervisión y auditoría".

Finalmente, es importante destacar que la Junta Monetaria tiene la atribución de normar lo referente a "operaciones y servicios financieros asociados a los medios de pagos electrónicos", por lo que las entidades que operen pasarelas deben estar atentas a estas regulaciones.

ANEXO 9: DEFINICIONES

a) **APIs** (Application Programming Interfaces / Interfaces de Programación de Aplicaciones): Son como "contratos" o "traductores" que permiten que diferentes programas de computadora se comuniquen e intercambien información entre sí de manera estandarizada.
b) **ARCO** (Derechos de Acceso, Rectificación, Cancelación y Oposición): Son los derechos que tienen las personas sobre sus datos personales, permitiéndoles acceder a ellos, corregirlos si son incorrectos, solicitar su eliminación o oponerse a su uso.
c) **Backoff Exponencial**: Una técnica utilizada en comunicaciones informáticas donde, si un intento de conexión o envío falla, se espera un tiempo antes de reintentar, y ese tiempo de espera aumenta progresivamente con cada nuevo fallo.
d) **CSV** (Comma-Separated Values / Valores Separados por Comas): Un formato de archivo simple para almacenar datos en forma de tabla, donde cada línea es una fila y los valores en cada fila están separados por comas.
e) **Client Credentials** Grant: Un método específico dentro de OAuth 2.0 que permite a una aplicación (cliente) obtener un token de acceso utilizando sus propias credenciales (identificador y secreto del cliente) para acceder a recursos protegidos en nombre propio, no de un usuario.
f) **Client Secret** (Secreto del Cliente): Una contraseña secreta conocida solo por la aplicación y el servidor de autorización, utilizada en el proceso de autenticación OAuth 2.0 para verificar la identidad de la aplicación.
g) **CRM** (Customer Relationship Management / Gestión de Relaciones con Clientes): Sistemas o software diseñados para ayudar a las empresas a gestionar y analizar las interacciones con sus clientes actuales y potenciales, con el objetivo de mejorar las relaciones comerciales.
h) **Dashboard** (Tablero de Control): Una interfaz visual que presenta información importante y métricas clave de forma resumida y fácil de entender, permitiendo monitorear el estado de un sistema o proceso.
i) **DDoS** (Distributed Denial of Service / Denegación de Servicio Distribuida): Un tipo de ciberataque en el que múltiples sistemas infectados (a menudo llamados "bots") se utilizan para sobrecargar un servidor o red con tráfico, haciendo que el servicio no esté disponible para los usuarios legítimos.
j) **Endpoint** (Punto Final): Una dirección web (URL) específica a la que una API envía solicitudes para realizar una operación o acceder a un recurso. Es el punto de entrada para la comunicación con un servicio web.
k) **ERP** (Enterprise Resource Planning / Planificación de Recursos Empresariales): Sistemas de software que ayudan a las organizaciones a gestionar y automatizar sus procesos de negocio principales, como finanzas, recursos humanos, manufactura, cadena de suministro, etc.
l) **Firma Digital**: Un mecanismo criptográfico que se utiliza para verificar la autenticidad e integridad de un documento o mensaje digital. Asegura que el documento proviene de quien dice ser y que no ha sido alterado desde que se firmó.
m) **FTP** (File Transfer Protocol / Protocolo de Transferencia de Archivos): Un conjunto de reglas estándar utilizado para transferir archivos entre computadoras a través de una red, como Internet.
n) **FTPS** (FTP Secure / FTP Seguro): Una extensión del protocolo FTP que añade una

capa de seguridad utilizando los protocolos SSL/TLS para cifrar las comunicaciones.

o) **GRC** (Gobernanza, Riesgo y Cumplimiento): Un enfoque integrado para gestionar la estrategia general de una organización (gobernanza), identificar y mitigar amenazas (riesgo), y asegurar el cumplimiento de leyes y regulaciones. El software GRC ayuda a automatizar y gestionar estos procesos.
p) **Hash** (Función Resumen): Un algoritmo matemático que toma una entrada (como un archivo o mensaje) y produce una cadena de caracteres de longitud fija, que es única para esa entrada. Se utiliza para verificar la integridad de los datos (asegurar que no han cambiado).
q) **HTTPS** (Hypertext Transfer Protocol Secure / Protocolo Seguro de Transferencia de Hipertexto): La versión segura del HTTP, el protocolo fundamental para la transmisión de datos en la World Wide Web. HTTPS cifra la comunicación entre el navegador del usuario y el sitio web para proteger la información.
r) **INDOTEL** (Instituto Dominicano de las Telecomunicaciones): El órgano regulador de las telecomunicaciones en la República Dominicana.
s) **Inyección** (Ataque de): Un tipo de ciberataque en el que se envían datos maliciosos a una aplicación para que ejecute comandos no deseados o acceda a información no autorizada.
t) **JSON** (JavaScript Object Notation / Notación de Objetos de JavaScript): Un formato ligero para el intercambio de datos, fácil de leer y escribir para los humanos, y fácil de interpretar y generar para las máquinas. Es comúnmente usado en APIs.
u) **JWS** (JSON Web Signature / Firma Web JSON): Un estándar para firmar digitalmente contenido utilizando JSON, asegurando la integridad y autenticidad del mensaje.
v) **Clave Privada / Clave Pública**: En criptografía, son un par de claves digitales relacionadas matemáticamente. La clave privada se mantiene secreta y se usa para firmar digitalmente o descifrar datos. La clave pública se puede compartir y se usa para verificar firmas digitales o cifrar datos que solo el poseedor de la clave privada puede descifrar.
w) **Microservicios**: Un enfoque para desarrollar software donde una aplicación grande se construye como un conjunto de servicios pequeños e independientes que se comunican entre sí, a menudo a través de APIs.
x) **MFA** (Multi-Factor Authentication / Autenticación Multifactor): Un método de seguridad que requiere que un usuario proporcione dos o más factores de verificación para acceder a un recurso, como una contraseña y un código enviado a su teléfono.
y) **NDAs** (Non-Disclosure Agreements / Acuerdos de Confidencialidad): Contratos legales entre dos o más partes que describen material, conocimiento o información confidencial que las partes desean compartir entre sí para ciertos propósitos, pero desean restringir el acceso a terceros.
z) **OAuth 2.0**: Un estándar abierto para la autorización delegada. Permite que aplicaciones de terceros accedan a recursos de un usuario en un servicio web sin necesidad de exponer las credenciales (como nombre de usuario y contraseña) del usuario a la aplicación de terceros.
aa) **ONAPI** (Oficina Nacional de Propiedad Industrial): La entidad gubernamental en la República Dominicana responsable del registro y protección de los derechos de propiedad industrial, como marcas y patentes.
bb) **OWASP** Top 10: Una lista, actualizada periódicamente por el Open Web Application

Security Project (OWASP), de los riesgos de seguridad más críticos para las aplicaciones web. Sirve como una guía para desarrolladores y profesionales de la seguridad.

cc) **PAdES** (PDF Advanced Electronic Signatures / Firmas Electrónicas Avanzadas para PDF): Un conjunto de restricciones y extensiones a PDF que lo hacen adecuado para firmas electrónicas avanzadas.

dd) **Payload** (Carga Útil): En el contexto de la transmisión de datos (como en una API), es la parte del mensaje que contiene los datos reales que se están enviando, excluyendo la información de encabezado o metadatos.

ee) **PCI-DSS** (Payment Card Industry Data Security Standard / Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago): Un conjunto de requisitos de seguridad diseñados para garantizar que todas las empresas que procesan, almacenan o transmiten información de tarjetas de crédito mantengan un entorno seguro.

ff) **PDF** (Portable Document Format / Formato de Documento Portátil): Un formato de archivo desarrollado por Adobe para presentar documentos, incluyendo texto y gráficos, de una manera independiente del software, hardware y sistema operativo.

gg) **PIN** (Personal Identification Number / Número de Identificación Personal): Un código numérico secreto utilizado para autenticar a un usuario en un sistema, comúnmente asociado con tarjetas bancarias.

hh) **Plantillas:** Corresponde a los modelos establecidos por esta Superintendencia para la remisión de información generada por las operaciones de las aseguradoras o reaseguradoras.

ii) **RNC** (Registro Nacional de Contribuyente): El número de identificación fiscal asignado a personas físicas y jurídicas en la República Dominicana para fines tributarios.

jj) **Scopes** (Ámbitos, en el contexto de tokens de acceso): En OAuth 2.0, los scopes definen el nivel de acceso que se otorga a un token. Limitan las acciones que una aplicación puede realizar en nombre de un usuario o en su propio nombre.

kk) **Servicios en la nube:** Serverless, o arquitectura sin servidor, es un modelo de computación en la nube donde el proveedor gestiona la infraestructura necesaria para ejecutar código. En lugar de aprovisionar y administrar servidores, los desarrolladores se enfocan en escribir y desplegar funciones específicas (funciones serverless) que se ejecutan bajo demanda y se escalan automáticamente.

ll) **Servicios Web:** Una forma de permitir que diferentes aplicaciones se comuniquen e intercambien datos a través de Internet utilizando estándares abiertos como HTTP, XML o JSON. Las APIs son una forma común de implementar servicios web.

mm) **SFTP** (SSH File Transfer Protocol o Secure File Transfer Protocol / Protocolo de Transferencia de Archivos Seguro): Un protocolo de red que proporciona funcionalidad de transferencia y manipulación de archivos sobre cualquier flujo de datos fiable. Se suele utilizar con el protocolo SSH para asegurar la transferencia.

nn) **SIPARD** (Sistema de Pagos y Liquidación de Valores de la República Dominicana): El sistema central en la República Dominicana para procesar pagos y liquidar transacciones de valores entre entidades financieras.

oo) **SIRIS** (Sistema de Remisión de Información de Seguros): El sistema implementado por la Superintendencia de Seguros de la República Dominicana para que las entidades aseguradoras y reaseguradoras envíen la información requerida.

pp) **SWIFT-CSCF** (SWIFT Customer Security Controls Framework / Marco de

Controles de Seguridad del Cliente de SWIFT): Un conjunto de controles de seguridad obligatorios y recomendados para los usuarios de la red SWIFT (una red global para mensajes financieros) para reforzar su ciberseguridad.

qq) **Token de Acceso** (Access Token): Una credencial digital que se utiliza para acceder a recursos protegidos en nombre de un usuario o aplicación. Es emitido por un servidor de autorización y presentado a un servidor de recursos para validar el acceso.

rr) **Trace_id** (Identificador de Traza): Un identificador único que se asigna a una solicitud o transacción a medida que se mueve a través de diferentes sistemas o servicios. Ayuda a rastrear y depurar problemas.

ss) **TLS** (Transport Layer Security / Seguridad de la Capa de Transporte): Un protocolo criptográfico diseñado para proporcionar comunicaciones seguras a través de una red informática. Es el sucesor de SSL (Secure Sockets Layer) y se utiliza ampliamente para asegurar las conexiones HTTPS.

tt) **XAdES** (XML Advanced Electronic Signatures / Firmas Electrónicas Avanzadas XML): Un conjunto de extensiones a XML-DSig que lo hacen adecuado para firmas electrónicas avanzadas.

uu) **XSS** (Cross-Site Scripting): Un tipo de vulnerabilidad de seguridad informática que se encuentra típicamente en aplicaciones web. Permite a los atacantes inyectar scripts maliciosos en páginas web vistas por otros usuarios.

vv) **XML** (Extensible Markup Language / Lenguaje de Marcado Extensible): Un lenguaje de marcado diseñado para transportar y almacenar datos. Es legible tanto por humanos como por máquinas y permite a los usuarios definir sus propias etiquetas.

ww) **XML-DSig** (XML Digital Signature / Firma Digital XML): Un estándar W3C para crear y verificar firmas digitales en documentos XML

ANEXO 10: BIBLIOGRAFIA

• Banco Central de la República Dominicana. (2018, 11 de mayo). *Certificación correspondiente a la Tercera Resolución adoptada por la Junta Monetaria en fecha 12 de abril del 2018, mediante la cual se autoriza la puesta en consulta de los sectores interesados del proyecto de Reglamento de Seguridad Cibernética y de la Información*.

• Congreso Nacional de la República Dominicana. (2002, 4 de septiembre). *Ley No. 126-02 sobre el Comercio Electrónico, Documentos y Firmas Digitales*. Promulgada por el Presidente Hipólito Mejía.

• Congreso Nacional de la República Dominicana. (2013, 13 de diciembre). Ley No. 172-13 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. Promulgada por el Presidente Danilo Medina. Publicada en la Gaceta Oficial No. 10737 el 15 de diciembre de 2013.

• Superintendencia de Seguros de la Republica Dominicana. (2024, 8 de enero). Resolución Num. 01/2024 sobre Requerimiento y Remisión de Información a la Superintendencia de Seguros. Firmada por la Superintendente Josefa A. Castillo Rodriguez.