



**IMPUESTOS  
INTERNOS**

**Especificaciones Técnicas - DGII-CCC-LPN-2022-0023**

**“Solución de Auditoria y trazabilidad de Datos”.**

**- Departamento de Seguridad de la Información y Monitoreo-**

## 1 Especificaciones Técnicas

### 1.1 Descripción de los Bienes.

Contar con una solución de seguridad, como mecanismo de auditoría, para aplicar controles de trazabilidad de cada uno de los XML o comprobantes electrónicos que están siendo recibidos y persistidos en los repositorios de los ambientes de factura electrónica, permitiendo el rastreo, visualización, análisis y la protección de datos no estructurados.

Esto con fines de detectar amenazas internas y posibles ciberataques analizando los datos, la actividad de las cuentas y el comportamiento de los usuarios; previniendo y limitando incidentes mediante el bloqueo de datos sensibles y obsoletos. Además, manteniendo un entorno automatizado y seguro con la gestión y reducción del riesgo.

Encontrar el mayor riesgo para la seguridad de datos es una tarea complicada, por lo que priorizar el riesgo, solucionar problemas de forma segura y mantener los datos protegidos requiere de una visibilidad considerable, ya que un gran porcentaje de las brechas de datos tardan meses o años en ser descubiertas, por lo que solo se necesita un punto final en riesgo para causar una importante brecha de datos si estos están sobreexposados y sin monitoreo.

A continuación, se describen los bienes de acuerdo con los lotes estipulados en la presente ficha:

Ítem	Descripción	Cantidad
1	Licencia por suscripción local (en premisa) con duración de 12 meses para 50 usuarios de Sistemas Operativos tipo UNIX/Linux.	50
2	Paquete de licencia para OneDrive y SharePoint Online por Suscripción local (en premisa) con duración de 12 meses para 500 usuarios.	500
3	Licencia por suscripción local (en premisa) duración de 12 meses para 750 usuarios de Sistemas Operativos tipo Microsoft Windows.	750
4	Licencia por suscripción local (en premisa) con duración de 12 meses para 750 usuarios.	750
5	Licenciamiento de clasificación de datos por suscripción local (en premisa) con duración de 12 meses para 50 usuarios de Sistemas Operativos Unix.	50
6	Licenciamiento de clasificación de datos para Sistemas Operativos tipo Microsoft Windows y SharePoint por Suscripción local (en premisa) con duración de 12 meses para 750 usuarios.	750
7	Licenciamiento de clasificación de datos para OneDrive y SharePoint Online por Suscripción local (en premisa) con duración de 12 meses para 500 usuarios.	500
8	Paquete de políticas de clasificación de datos por Suscripción local (en premisa) con duración de 12 meses para 750 usuarios.	750
9	Etiquetas de clasificación de datos por Suscripción local (en premisa) con duración de 12 meses para 750 usuarios.	750
10	Licenciamiento bajo modalidad por Suscripción con duración de 12 meses de un collector local (en premisa).	1
11	24 horas de Servicios Profesionales	3

### 1.1.1 Requerimientos del Proveedor

Ítem	Descripción								
RP01	El proveedor deberá atender y resolver cualquier problema técnico de la solución, en un esquema de atención 8 x 5 X 365 (telefónico, e-mail, acceso remoto o presencial en caso de que la entidad así lo requiera).								
RP02	El oferente debe prestar asistencia ante un incidente de acuerdo con el siguiente esquema: <table border="1" data-bbox="389 629 1299 808"> <thead> <tr> <th>Nivel de Severidad</th> <th>Tiempo de Respuesta</th> </tr> </thead> <tbody> <tr> <td>Severidad 1</td> <td>4 horas durante horas laborables</td> </tr> <tr> <td>Severidad 2</td> <td>6 horas durante horario laborable</td> </tr> <tr> <td>Severidad 3</td> <td>1 Día, durante días laborables</td> </tr> </tbody> </table>	Nivel de Severidad	Tiempo de Respuesta	Severidad 1	4 horas durante horas laborables	Severidad 2	6 horas durante horario laborable	Severidad 3	1 Día, durante días laborables
Nivel de Severidad	Tiempo de Respuesta								
Severidad 1	4 horas durante horas laborables								
Severidad 2	6 horas durante horario laborable								
Severidad 3	1 Día, durante días laborables								
RP03	Los trabajos de instalación, implementación u otros servicios de soporte serán realizados en la Sede Central de la DGII.								

### 1.1.2 Requerimientos Técnicos

Número	Descripción
RT01	La solución deberá permitir su gestión en forma centralizada. La provisión de dicha funcionalidad deberá suministrar la posibilidad de ser realizada mediante un canal seguro, local y remoto.
RT02	La solución deberá permitir como mínimo 8 usuarios concurrentes para la administración y operación de la solución.
RT03	La solución deberá suministrar identificación y autenticación simple de usuarios e integrable con Active Directory/ LDAP.
RT04	La solución deberá facilitar la segregación de funciones entre los roles indicados permitiendo el siguiente nivel de granularidad: capacidad de operar, consultar y administrar.
RT05	La solución deberá suministrar un módulo de auditoría que registre y reporte la actividad realizada en la administración y uso de la mi5sma, incluyendo inicio y cierre de sesión y trazabilidad de las acciones de los usuarios de la solución, registro de eventos del ciclo de vida de los usuarios de la solución, registro de todos los eventos asociados a los usuarios de la solución y registro de eventos del ciclo de vida de las reglas de auditoría administradas por la solución.
RT06	La solución deberá garantizar la operación normal de los sistemas monitoreados, aún frente a fallas en el funcionamiento de la solución, sin afectar la operación de los sistemas monitoreados.
RT07	Si se requiere instalar un software del tipo agente, La solución deberá garantizar el mínimo impacto en el rendimiento de los equipos monitoreados, debiendo impactar al desempeño de éstos en menos de un 5% y no se deberá requerir el reinicio de dichos equipos para su instalación.

Número	Descripción
RT08	La solución no deberá implementar función de los logs nativos de los contenedores o file servers a monitorear, y en caso de cortes de conexión la solución deberá contar con un buffer que le permita almacenar la información de eventos sin sobrescribirlos.
RT09	Visualización de logs mediante una interfaz gráfica de administración y seguimiento detallado. Deberá permitir efectuar un análisis en tiempo real de los registros de eventos, brindando facilidades de explotación
RT10	Los reportes programados deben poderse enviar mediante correo electrónico a diferentes destinatarios e incluir el adjunto en formatos como Excel, PDF, HTML, o CSV como mínimo.
RT11	La solución deberá permitir granularidad en la generación de reportes personalizados, generados bajo demanda o de forma automática, que satisfaga una combinación de todas las variables y atributos que provea la solución y generación de reportes estadísticos. Estos deberán poder exportarse a múltiples formatos como PDF, XLS, HTML y CSV como mínimo
RT12	La solución deberá permitir visibilidad gráfica de permisos por cada objeto, usuario o grupo de todas las carpetas donde el usuario o grupo tiene permiso de acceso.
RT13	El consumo de recursos en los sistemas monitoreados no debe afectar las diferentes aplicaciones y roles en ejecución en dicha plataforma.
RT14	La solución deberá permitir una visibilidad gráfica de la configuración de permisos, incluyendo herencia on/off (protección), singularidad, y compartido/no compartido, de forma interactiva. Además de filtros para ver solo ciertos objetos, incluyendo carpetas protegidas o únicas.
RT15	La solución debe permitir en una sola interfaz gráfica para todas las plataformas monitoreadas, supervisar la visibilidad bi-direccional y multi-nivel de los directorios que pueden ser accedidos por los usuarios y en la dirección opuesta, mostrando todas las carpetas en las que tiene acceso el usuario e identificando qué tipo de acceso es (lectura, escritura, modificación).
RT16	La solución debe identificar los permisos excesivos basados en el análisis de los eventos de auditoría
RT17	Visibilidad completa de los permisos de usuarios, grupos y carpetas de los sistemas de archivos (carpetas de recursos compartidos).
RT18	Lista de auditoria detallada de cada evento de acceso, por usuario o por carpeta.
RT19	Capacidad de la solución para recomendaciones acerca del punto en donde los permisos excesivos pueden ser removidos y la habilidad de simulación de cambios sin afectar la producción.
RT20	La solución de software debe permitir agregar usuarios y permisos a los datos y carpetas, de manera granular o específica, por grupos o usuarios específicos.
RT21	Identificación de la propiedad de datos a través del análisis de la actividad del usuario.
RT22	Arquitectura extensible para incluir otros metadatos, funcionalidades y plataformas.
RT23	Identificar automáticamente a los propietarios de datos para incluirlos en procesos de gobierno de datos.
RT24	Se requiere administrar el derecho y acceso de manera eficiente y efectiva.
RT25	Auditar el acceso a cada archivo.
RT26	Se requiere proveer inteligencia crítica para el personal de TI, acerca de quién puede y quién está teniendo acceso a los datos, quién es el propietario de los datos, y en qué lugar puede reducirse el acceso a los datos de manera fácil, sin afectar los procesos de negocio.

Número	Descripción
RT27	La solución deberá tener capacidad de análisis de comportamiento de los usuarios sobre información obsoleta de la Entidad.
RT28	Detección y Análisis de comportamientos inusuales sobre datos no estructurados.
RT29	Capacidad de Identificar comportamiento anormal causado por ataques de ransomware, incluso en sus etapas tempranas, integrada dentro de la misma solución
RT30	Identificación de patrones de actividad inusual en los recursos compartidos en los diferentes servidores de archivo.
RT31	Proporcionar informes de SID inconsistentes en ACLs, y ACE de usuarios Individuales en ACL's.
RT32	Proporcionar informes de datos o usuarios inactivos de una plataforma monitoreada.
RT33	Proporcionar informes de usuarios deshabilitados que aún están en grupos de seguridad en un dominio específico.
RT34	Uso del Active Directory como medio de autenticación y control de acceso de la Solución.
RT35	Deberá tener la capacidad de importar los diferentes datos adicionales del active directory en los reportes creados, como por ejemplo descripción, departamento, correo electrónico, OU entre otros.
RT36	Deberá contar con alertas que se puedan enviar vía SNMP.
RT37	Deberá contar con la capacidad de ejecutar comandos de powershell en caso de ser requerido cuando una alerta sea generada.
RT38	Trazabilidad de la actividad total de usuarios y de cambios realizados en la información no estructurada.
RT39	Control de permisos sobre usuarios y grupos.
RT40	Control de permisos sobre de archivos y carpetas.
RT41	Generación de reportes parametrizables.
RT42	Permitir dar visualización bidireccional de permisos (usuario-carpeta, carpeta-usuario) de las asociaciones y privilegios de los usuarios y su alcance.
RT43	Registrar toda actividad que ocurra en archivos y carpetas: abrir, crear, remover, modificar, mover, identificando nombre de usuario, archivo impactado, ruta, nueva locación, hora de la actividad, número de veces de la actividad realizada entre otros.
RT44	Proporcionar una visibilidad gráfica de la actividad de acceso de los archivos y carpetas.
RT45	Proporcionar un filtro gráfico, para ordenar y agrupar los diferentes tipos de eventos y búsquedas.
RT46	Proporcionar informe de actividades de acceso de los archivos, carpetas, usuarios, grupos de seguridad.
RT47	No debe tener dependencia de auditoría nativa del sistema operativo para servidores de archivos Windows.
RT48	Proporcionar niveles altos, visibilidad de resumen gráfico de actividad auditada, incluyendo: <ul style="list-style-type: none"> <li>• vista de los usuarios con mayor y menor actividad</li> <li>• vista de los directorios con mayor y menor actividad</li> <li>• vista de directorios que un usuario o grupo haya accedido</li> <li>• vista de usuarios que han estado acezando un directorio</li> </ul>
RT49	Proporcionar informes personalizados, por demanda y programados con la capacidad de agregar filtros, condiciones, campos adicionales
RT50	Proporcionar la identificación gráfica de niveles de actividad de acceso inusual a datos críticos, de acuerdo con niveles de categorización configurados previamente

Número	Descripción
RT51	Proporcionar informes de actividad de acceso inusual, identificando los diferentes tipos de eventos que están fuera la actividad habitual de un usuario (s).
RT52	Proporcionar informe de administradores acezando datos del negocio, por demanda y programado con datos como fecha, número de veces, detalles del acceso (exitoso o fallido) entre otros
RT53	Proporcionar utilidades gráficas para retroactivamente simular el efecto de cambios de permisos ó membresía de grupo basado en historia de eventos de acceso.
RT54	Capacidad de realizar simulaciones previas a un cambio de permisos sobre grupo de seguridad o usuarios conociendo el impacto de dicho cambio antes de aplicarlo en producción
RT55	Proporcionar informe incluyendo objetos de datos cuyos permisos están expuestos a grupos de "acceso global" como everyone, usuarios de dominio, usuarios autenticados, y quién está usando activamente esos permisos para acceder a los datos
RT56	Capacidad de rectificar permisos y realizar cambios a grupos desde una interfaz gráfica directa en la solución.
RT57	Almacenar todos los cambios a permisos hechos dentro de la consola de administración y fuera de la consola (directamente en las plataformas monitoreadas).
RT58	Registrar todos los cambios de membresía de grupo hechos 'dentro de' y 'fuera de' la consola de gestión
RT59	Debe tener un método de asignar o asociar un usuario como un "propietario" de datos según el uso y cantidad de eventos.
RT60	Generar informes en demanda y programados a propietarios asignados sobre sus objetos de datos y grupos, incluyendo permisos, actividad de acceso, estadísticas de acceso y cambios en permisos.
RT61	Proporcionar un método para que los propietarios de datos reciban automáticamente un reporte de actividad de una carpeta específica incluyendo eliminación, creación, apertura de archivos.
RT62	Debe tener un método grafico para identificar el top de usuarios con mayor actividad en una ruta o carpeta específica por periodo de tiempo determinado
RT63	Poseer un método grafico para identificar los usuarios con más alertas de actividad generadas en un periodo específico
RT64	Proporcionar soporte para instalación remota de agentes de auditoría
RT65	La recolección de eventos no debe almacenar archivos temporales en los sistemas monitoreados causando aumento en I/O y afectando el rendimiento de dichos sistemas.