CONSEJO NACIONAL DE SEGURIDAD SOCIAL
SOLICITUD DE COMPRA O CONTRATACIÓN
UNIDAD OPERATIVA DE COMPRAS Y CONTRATACIONES

DATOS GENERALES			
NOMBRE DEL SOLICITANTE:	**Pedro Rossi**		
ÁREA:	**Dirección de Tecnologías de la Información y Comunicación**	**FECHA:**	**28/06/2023**
OBJETO DE LA COMPRA:	**Software para Backup, Replicacion y Recuperacion de Desastres.**		

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANTIDAD SOLICITADA
1	Software backup, replicacion y recuperacion de desastres para toda la infraestructura de servidores de la institución.	Unidad	1

ESPECIFICACIONES TÉCNICAS:

Ver fichas tecnicas adjuntas.

PLAN DE ENTREGA ESTIMADO (ALINEACIÓN POA-PACC-PRESUPUESTO)			
FECHA ESTIMADA DE ENTREGA:	07 días hábiles, luego de la emisión de la orden de compras	**HORA DE ENTREGA:**	09:00 a.m
LUGAR DE ENTREGA:	**Piso 11, La Cumbre.**		

PLANIFICACION OPERATIVA ANUAL			
ALINEACIÓN POA-PACC-PRESUPUESTO.	**PROGRAMACIÓN:** ☑ POA ☑ PACC ☑ Presupuesto	**DESCRIPCIÓN DE LA ACTIVIDAD PROGRAMADA:**	Cronograma de aquisición y renovación de licenciamiento de software y elaboración de TDR´s.
	ACTIVIDAD NO PROGRAMADA: ☐ **(Justifique la Compra)**		

VERIFICACIÓN Y VALIDACION POR DPD			
CÓDIGO ACTIVIDAD POA:	**DTIC.5.20.2.2.62**	**CUENTAS PRESUPUESTARIAS:**	
FIRMA, FECHA Y SELLO (DPD):	04/07/2023		

AUTORIZACION

Unidad Solicitante
Firma y Sello

Dirección Administrativa
Firma y Sello

Gerente General
Firma y Sello

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

FORMULARIO DE ESPECIFICACIONES TÉCNICAS PARA LA ADQUISICIÓN DE EQUIPOS, SOFTWARES Y/O MATERIALES TECNOLÓGICOS

INFORMACIONES DE ACUERDO AL RECURSO TECNOLÓGICO	
Componentes	**Caracteristicas Generales**
Recurso Tecnológico:	Software para Backup, Replicacion y Recuperacion de Desastres.
Descripción del Recurso:	Software backup, replicacion y recuperacion de desastres para toda la infraestructura de servidores de la institución.
Cantidad:	1
Tipo de Licenciamiento	Perpetuo
Alcance del Licenciamiento	Para entorno de 14 servidores virtuales y 6 servidores fisicos.
Mantenimiento, Soporte y Actualización	1 año 7x24 o superior
Respaldo basado en snapshots de VMs VMware y Hyper-V.	La solución debe proporcionar una copia de seguridad eficiente 'incremental para siempre' e incluir opciones de copias de seguridad completas y ad-hoc.
	La solución debe admitir la copia de seguridad de VM directamente desde SAN.
	La solución debería detectar automáticamente las máquinas virtuales con el uso compartido de bus SCSI y excluirlas de la copia de seguridad.
	La solución debería detectar automáticamente el espacio libre del datastore productivo y evitar el snapshot de copia de seguridad si el espacio está por debajo del umbral definido.
	La solución debería monitorear automáticamente la latencia del datastore productivo durante la copia de seguridad y reducir la velocidad de la copia de seguridad si la latencia del datastore supera un umbral definido.
	La solución debería detectar automáticamente los snapshots de VMware huérfanas y eliminarlas.
	La solución debería permitir la exclusión de discos de máquinas virtuales y archivos de intercambio (swap) en copias de seguridad basadas en snapshots.
	La solución debería permitir la exclusión de archivos y carpetas de la copia de seguridad basada en snapshots.
	La solución deberá permitir la exclusión de los bloques marcados como eliminados para reducir el tamaño de la copia de seguridad y aumentar el rendimiento del respaldo.
	La solución no debería requerir agentes implementados en máquinas virtuales para facilitar el respaldo de aplicaciones y la recuperación granular.
	La solución no debe necesitar realizar copias de seguridad de sistema operativo separadas de las copias de seguridad de datos de la aplicación en máquinas virtuales para facilitar la recuperación granular de elementos de la aplicación.
	La copia de seguridad sin agente de máquinas virtuales debe truncar los registros de transacciones o archivos de Microsoft SQL, Microsoft Exchange y Oracle Database.
	La copia de seguridad sin agente de máquinas virtuales debe proporcionar copias de seguridad de registros o archivos de transacciones de Microsoft SQL, Oracle Database y PostgreSQL junto con copias de seguridad basadas en snapshots.
	La solución debería permitir la recuperación de archivos y elementos de aplicaciones sin instalar Agentes o plugins en Máquinas Virtuales.
Respaldo de VMware con integraciones de snapshot de almacenamiento	La solución debe integrarse con los sistemas de almacenamiento y utilizar snapshots de almacenamiento para las operaciones de respaldo.
	La solución debería poder leer los datos de la máquina virtual directamente desde un snapshot de almacenamiento a través de una conexión SAN.
	La solución deberá proporcionar la capacidad de explorar máquinas virtuales en snapshots de almacenamiento y recuperar instantáneamente la máquina virtual, el archivo del sistema operativo o la carpeta o los elementos de la aplicación directamente desde el snapshot de almacenamiento. Esta capacidad también debería aplicarse a los snapshots de almacenamiento creados independientemente de la aplicación de respaldo.
	La solución deberá poder utilizar snapshots de almacenamiento para crear una copia de la máquina virtual en un entorno de red aislado para fines de prueba.

Protección de datos continua para VMware (CDP)	La solución deberá replicar máquinas virtuales sin snapshots del ambiente virtual y debe capturar todas las E/S de escritura directamente del disco de la VM.
	La solución no deberá tener dependencia de hardware y deberá proteger cualquier S.O. y Aplicación que corra en una VM de vSphere, sin importar si se ejecuta en infraestructuras convergentes, hiperconvergentes o discos locales del vSphere ESXi.
	La solución deberá ser una replicación asíncrona que se pueda utilizar sin limitación de distancia.
	La funcionalidad deberá estar incluida en el mismo licenciamiento de respaldo, es decir que no debe requerir alguna otra licencia adicional.
Ofrecerá un respaldo basado en agente de entornos físicos	La solución debe admitir copias de seguridad físicas de sistemas operativos Windows, Linux, UNIX y MAC.
	La solución debería facilitar la copia de seguridad a nivel de imagen y de archivo de entornos físicos o basados en la nube.
	La solución debe utilizar la tecnología Changed Block Tracking para copias de seguridad incrementales de cargas de trabajo físicas o basadas en la nube.
	La solución debe admitir la copia de seguridad de los servidores de Windows configurados como clúster.
	La solución debe proporcionar complementos de respaldo para las aplicaciones MS SQL, Oracle RMAN y SAP HANA, permitiendo la centralización de repositorio.
	La solución debe proporcionar conocimiento de la aplicación al realizar copias de seguridad de MySQL y PostgreSQL que se ejecutan en Linux.
	La solución debe permitir mover los archivos de respaldo entre cualquier tipo de repositorio de respaldo (aun cuando el repositorio destino sea de un tipo distinto al del origen) sin necesidad de usar la gestión regular de archivos (copiar/pegar).
	La solución debe permitir mover los respaldos entre las tareas y copiar los respaldos entre repositorios.
Recuperación de VMs VMware \ Hyper-V y servidores físicos	La solución debe proporcionar una portabilidad completa en cualquier archivo de respaldo propietario y no debe depender de ninguna infraestructura de respaldo como por ejemplo, el catálogo central, para la recuperación.
	La solución debe proporcionar tecnología de recuperación de la máquina virtual snapshot, correr múltiples Virtual Machine directamente desde el servidor de copia de seguridad del repositorio.
	La solución debe proporcionar la tecnología de recuperación Changed Block Tracking para máquinas virtuales VMware, Hyper-V y Nutanix AHV.
	La solución debe permitir que las copias de seguridad de máquinas virtuales en la nube puedan ser restauradas en cualquier nube pública o volver a una máquina virtual en un hipervisor local en las instalaciones.
	La solución debería permitir la recuperación de VMware Virtual Machine a través del canal de fibra SAN.
	La solución debe escanear los datos de la máquina virtual con un software antivirus antes de restaurar la máquina al entorno de producción. La solución debería abortar la operación de recuperación si se detecta malware.
	La solución debería proporcionar la capacidad de iniciar la máquina virtual en un entorno de red aislado durante el proceso de recuperación e inyectar un script en el sistema operativo invitado que permita que el servidor se modifique para fines de cumplimiento antes de la recuperación.
	La solución debería proporcionar una recuperación completa de la copia de seguridad basada en el Agente con la capacidad de crear un medio de arranque para el servidor específico, del tipo bare metal.
	La solución debe permitir la recuperación instantánea de copias de seguridad basadas en agentes para VMware o máquinas virtuales Hyper-V.
	La solución debe permitir la recuperación instantánea de copias de seguridad de sistemas de archivos tipo NAS (FileShares).
	La solución debería facilitar la recuperación de VMware o una copia de seguridad basada en agentes directamente en Google Platform, Amazon AWS o Microsoft Azure y Microsoft Azure Stack.
	La solución debería convertir automáticamente UEFI a BIOS durante la operación de recuperación de Amazon AWS.

Recuperación a nivel de archivo	La solución debería facilitar las operaciones de recuperación a nivel de archivo sin la necesidad de implementar un agente o plugin de recuperación en un servidor virtual o físico.
	La solución debería poder recuperar archivos en un sistema operativo invitado de máquina virtual incluso cuando no haya conexión de red entre el servidor de respaldo y la máquina virtual.
	La solución debe permitir delegar operaciones de restauración y proporcionar una interfaz de usuario de autoservicio basada en la web y la capacidad de buscar máquinas, recursos compartidos de archivos y archivos específicos en todas las copias de seguridad.
	La solución debe admitir todos los sistemas de archivos.
	La solución debe permitir restaurar las listas de control de acceso (ACL) de archivos y carpetas sin la necesidad de sobre escribir los archivos.
Recuperación de elementos de aplicación	La solución debería admitir la recuperación granular de las aplicaciones de Microsoft Active Directory, Exchange, SQL, SharePoint y PostgreSQL.
	La solución debería admitir la recuperación granular de bases de datos Oracle a partir de copias de seguridad basadas en imágenes u Oracle RMAN.
	La solución no debe usar un producto de terceros para la recuperación granular de elementos de la aplicación.
	La solución debe proporcionar una interfaz de usuario de autoservicio basada en la web y la capacidad de examinar y recuperar elementos de Microsoft Exchange y bases de datos SQL u Oracle.
	La solución debe permitir la recuperación instantánea de base de datos SQL u Oracle desde la copia de seguridad al último estado o a un punto anterior en el tiempo a cualquier servidor de base de datos de producción o clúster (físico o virtual) en minutos, independientemente de su tamaño.
Copia de seguridad en disco	La solución debe estar definida por software y ser capaz de ejecutarse localmente o en cualquier plataforma en la nube.
	La solución debe ser independiente del almacenamiento y debe contar con tecnología integrada de deduplicación y compresión.
	La solución deberá asegurar las copias de seguridad en repositorios reforzados a prueba de malware y hackers con copias de seguridad inmutables, para prevenir el cifrado o eliminación por ransomware y debe admitir credenciales que se usan una sola vez y no ser almacenadas en la infraestructura de respaldo, así si el servidor de respaldo se ve comprometido, un atacante no puede obtener las credenciales y conectarse al repositorio reforzado.
	La solución debe poder escalar tanto horizontal como verticalmente.
	La solución debe proporcionar un mecanismo fácil para expandir o contratar el almacenamiento de respaldo de destino.
	La solución debería ofrecer la flexibilidad para ajustar el tamaño del bloque de deduplicación de datos y el nivel de compresión de datos.
	La solución debe integrarse con los dispositivos de deduplicación EMC Data Domain, HPE Store Once, Quantum, ExaGrid, Fujitsu, Hitachi e Infinidat.
Copia de seguridad en cinta	La solución debería admitir de forma nativa la copia del respaldo a cinta y no debería requerir software adicional para su administración.
	La solución debe admitir copias de seguridad deduplicadas y comprimidas en medios de cinta.
	La solución debe admitir medios de cinta WORM.
	La solución no debe requerir licenciamiento adicional para el uso de librerías sin importar la cantidad de drives que tengan.
Repositorio y Copia de seguridad en la nube	La solución debería admitir de forma nativa como repositorio y el traslado de archivos de respaldo a Amazon S3 (con inmutabilidad), IBM Cloud Object Storage, Azure Blob Cloud Storage (con inmutabilidad), Google Cloud Storage, y otras plataformas de almacenamiento en la nube compatibles con S3.
	La solución debería admitir de forma nativa el traslado de archivos de respaldo a Amazon S3 Glacier (incluido Deep Archive) con capacidad de inmutabilidad, y Microsoft Azure Blob Storage Archive Tier para archivado a largo plazo de copias de seguridad

Repositorio y Copia de seguridad en la nube	La solución debe proporcionar una recuperación incremental y granular del almacenamiento de objetos basado en la nube.
	La solución debe proporcionar soporte para el almacenamiento de objetos en las instalaciones.
	La solución debe ofrecer un movimiento incremental de datos hacia y desde el almacenamiento basado en objetos.
	La solución debería ofrecer inmutabilidad en el almacenamiento de objetos S3 a nivel de depósito.
	La solución debe tener la opción de copiar o mover datos al almacenamiento de objetos al finalizar la copia de seguridad. Idealmente, ambas opciones se pueden combinar.
Seguridad de datos de respaldo	La solución debería encriptar los archivos de respaldo usando el encriptado AES de 256 bits. El cifrado no debe depender de la plataforma de almacenamiento de respaldo.
	La solución debe proporcionar un cifrado AES de 256 bits con tecnología de protección de pérdida de contraseña, por lo que los datos se pueden descifrar si se pierde la contraseña operativa.
	Todos los componentes de la solución de respaldo deben admitir autenticación Kerberos.
	La solución debe integrarse con autenticación de credenciales del tipo gMSA.
	La solución debe permitir autenticación multifactor (MFA) para una verificación adicional de usuario en la consola de administración de la solución.
	La solución debe integrarse con SAML 2.0 para la autenticación extendida.
	La solución debe proporcionar control de acceso basado en roles a través de una interfaz de usuario web para la mayoría de las operaciones de recuperación y respaldo.
Verificación de datos de respaldo	La solución debería leer y verificar automáticamente la consistencia de los datos de producción en el archivo de copia de seguridad una vez completada la copia de seguridad. En caso de que se detecte corrupción de datos, la solución debería reconstruir automáticamente el bloque dañado con datos de producción.
	La solución deberá iniciar automáticamente las máquinas virtuales de VMware y Hyper-V Windows y Linux así como de agentes de nube y físicas a partir de copias de seguridad y verificar el sistema operativo y la disponibilidad de la aplicación. Esta prueba no debe tener impacto en la red de producción. La solución debe proporcionar un informe de verificación de recuperación.
	La solución debería escanear automáticamente los datos de producción en busca de virus durante la verificación de respaldo.
Copia de seguridad NAS	La solución debe proporcionar una copia de seguridad eficiente basada en archivos incrementales.
	La solución debe admitir recursos compartidos de archivos basados en NFS, SMB, Windows y Linux.
	La solución debe aprovechar los snapshots basadas en matrices para copias de seguridad basadas en archivos siempre que sea posible.
	La solución debe aprovechar los snapshots de VSS cuando sea posible.
	La solución debe proporcionar una recuperación incremental a cualquier plataforma objetivo-heterogénea.
	La solución debe proporcionar un mecanismo de reversión incremental para cualquier recurso compartido NAS.
	La solución debe proporcionar la capacidad de archivo granular de archivos, archivando tipos de archivos específicos.

Operaciones de respaldo en entorno nube	La solución debe estar desarrollada para tareas de protección y recuperación ante desastres para entornos Amazon Elastic Compute Cloud (EC2), Amazon Relational Database Service (RDS) y Amazon Elastic File System (EFS). También debe permitir respaldar y restaurar las configuraciones de Amazon Virtual Private Cloud (VPC).
	La solución debe poder realizar las siguientes operaciones de protección de datos: crear instantáneas nativas de la nube de instancias EC2, crear instantáneas nativas de la nube de los recursos de RDS, crear copias de seguridad a nivel de imagen de instancias EC2 y crear copias de seguridad de los sistemas de archivos EFS.
	La solución debe poder realizar las siguientes operaciones de recuperación de datos respaldados: restaurar instancias EC2 completas, restaurar volúmenes de instancias EC2, restaurar archivos y carpetas de instancia EC2, restaurar instancias de base de datos de RDS, restaurar sistemas de archivos EFS completos, así como archivos y directorios EFS, configuraciones completas y elementos específicos de configuraciones de VPC.
	La solución debe estar desarrollada para tareas de protección y recuperación ante desastres para entornos de Microsoft Azure.
	La solución de poder realizar las siguientes operaciones: crear copias de seguridad a nivel de imagen e instantáneas nativas de la nube de máquinas virtuales de Azure, crear copias de seguridad a nivel de imagen de las bases de datos de Azure SQL, crear instantáneas nativas en la nube de recursos compartidos de archivos de Azure, restaurar archivos individuales de recursos compartidos de archivos de Azure, bases de datos específicas de Azure SQL, máquinas virtuales de Azure completas, discos virtuales individuales y archivos y carpetas del sistema operativo invitado.
	La solución debe estar desarrollada para tareas de protección y recuperación ante desastres para entornos de Google Cloud.
	La solución de poder realizar las siguientes operaciones: crear copias de seguridad a nivel de imagen e instantáneas nativas de la nube de instancias de máquinas virtuales de Google, crear copias de seguridad a nivel de imagen e instantáneas nativas de la nube de las instancias de Google Cloud SQL, restaurar instancias de Google Cloud SQL completas, bases de datos de Google Cloud SQL específicas, instancias de máquinas virtuales de Google completas, discos persistentes individuales y archivos y carpetas del sistema operativo invitado.
Monitoreo y Reporteria de Respaldo	La solución debe proporcionar información del estado de protección de cargas de trabajo virtuales, físicas o basadas en nube.
	La solución debe alertar sobre trabajos de respaldo fallidos y trabajos que exceden la ventana de respaldo.
	La solución debe alertar por adelantado si el objetivo de la copia de seguridad se acerca a la capacidad.
	La solución debe proporcionar alertas proactivas para eliminar problemas. Estos problemas deben detectarse automáticamente, abarcar la configuración y el rendimiento, y el proveedor debe actualizar dinámicamente la detección.
	La solución debe proporcionar un informe de evaluación de Infraestructura VMware para asegurar que el entorno esté preparado para las operaciones de respaldo basadas en snapshots y detectar máquinas virtuales que requieren implementación de respaldo basada en agente.
	La solución debe proporcionar un informe de autoevaluación. El informe debe detectar si la solución se implementa de acuerdo con las mejores prácticas.
	La solución debe proporcionar un informe sobre máquinas virtuales que no están protegidas por copia de seguridad y un informe de cumplimiento de RPO (Objetivo del punto de recuperación) para las máquinas virtuales protegidas.
	La solución debe proporcionar planificación de capacidad y pronosticar la utilización del espacio de almacenamiento de respaldo.
	La solución debe proporcionar un informe automatizado sobre todas las operaciones de recuperación para fines de auditoría.
	La solución debe proporcionar una infraestructura de respaldo y un informe de cambios de política para fines de auditoría.
	La solución debe permitir definir dashboards de monitoreo personalizados e integraciones con sistemas ITSM con la ayuda de REST APIs.
	La solución debe permitir programar la entrega automática de dashboards, informes y carpetas de informes. Se debe poder optar por recibir dashboards e informes por correo electrónico, guardar dashboards e informes en una carpeta local o recurso compartido de red.
	La solución debe notificar a los usuarios sobre eventos importantes, cambios y posibles problemas en el entorno virtual y de copia de respaldo.
	La solución debe ser capaz de tomar acciones de remediación como por ejemplo ejecutar un script que encienda una VM, o ejecutar un script que agregue una VM a un trabajo de respaldo existente o ejecutar un script que elimine el último snpashot en VMware o que elimine el último checkpoint en HyperV.

Orquestación de Recuperación de Desastres	La solución debe permitir la orquestación de procesos de recuperación, con planes de orquestación de un solo clic para aplicaciones críticas.
	La solución debe crear flujos de trabajo de recuperación ante desastres, automatizar procesos de recuperación y eliminar pasos manuales propensos a errores.
	La solución debe proporcionar capacidades de generación de informes que permitan documentar los planes de recuperación ante desastres para cumplir con los requisitos de auditoría.
	La solución debe crear flujos de trabajo para organizar operaciones de recuperación para máquinas virtuales y físicas en entornos de nube de VMware vSphere y Microsoft Azure como mínimo.
	La solución debe permitir programar los controles y las pruebas para automatizar la verificación de los planes de orquestación, con funciones como laboratorios de prueba aislados y controles integrales de preparación.
	La solución debe permitir ver los logros de RPO y RTO en un dashboard y generar informes actualizados automáticamente para las verificaciones, pruebas y ejecuciones del plan de orquestación que garanticen que se cumplan los requisitos de cumplimiento y auditoría.
Otros requerimientos	La solución debe proporcionar la tecnología de migración de máquina virtual VMware donde la máquina virtual se puede migrar a través de clústeres y centros de datos de VMware y entre centros de datos físicos.
	La solución debería poder utilizar la copia de seguridad o réplica de la máquina virtual para crear una copia de la máquina virtual en un entorno de red aislado para fines de prueba.
	La solución debe presentar la tecnología de replicación de máquina virtual VMware con la capacidad de configurar el failover y el failback, convertir en tiempo real el tipo de disco de la máquina virtual de thin a thick y viceversa y deshacer la operación de recuperación de fallas o recuperación de fallas, incluido en la licencia de respaldo y misma consola.
	La solución debe incluir un mecanismo de copia de seguridad fuera del sitio con la capacidad de seleccionar individualmente los conjuntos de copias de seguridad que deben copiarse y definir una retención diferente de las copias de seguridad en el almacenamiento secundario de copias de seguridad.
	La solución debe presentar tecnología de aceleración WAN incorporada para la replicación de datos con la capacidad de limitar la utilización del ancho de banda.
Servicios	Despliegue
	Implementación completa de solución de Backup
	Puesta a punto, llave en mano
Reconocimiento de la Marca	La marca debe ser reconocida a nivel internacional con más de 10 años de comercialización en el país y tener representación oficial local.
Ensamblaje	Los componentes internos que hacen parte del portafolio de la marca deben ser ensamblados desde fábrica.
Accesorios	La marca fabricante deberá contar con accesorios de marca propia, disponibles y compatibles con el equipo ofertado.
Otros	No se aceptarán equipos remanufacturados, o con piezas de diferentes fabricantes.
Certificación del Oferente sobre la solución Ofertada (Servicios)	Certificado para la venta
	Certificado para la instalación/configuración de los Equipos/Servicios (Implementación)
	Certificado para dar Soporte
Nota:	Se debe anexar la ficha técnica y cualquier otra documentación oficial (fabricante) o evidencia que compruebe que los equipos, componentes, piezas, partes o servicios ofertados cumplen con las caracteristicas requeridas.
********** NO EXISTE MAS INFORMACION DEBAJO DE ESTA LINEA**********	

Revisado y Aprobado Por:

Pedro Rossi
Director TIC
28/06/2023
Fecha

CONSEJO NACIONAL DE SEGURIDAD SOCIAL
CNSS
Dirección TIC
Santo Domingo, R.D.