FORMULARIO DE EVALUACIÓN DE PROPUESTA TÉCNICA
CONSEJO DEL PODER JUDICIAL

FORMULARIO DE EVALUACIÓN PROPUESTA TÉCNICA	
Nombre del Proceso	CONTRATACIÓN DE LOS SERVICIOS DE MONITOREO Y RESPUESTA A INCIDENTES CIBERNÉTICOS
Referencia del Proceso	**CP-CPJ-BS-12-2022**
Fecha de Evaluación	06 DE SEPTIEMBRE DE 2022
Oferente	**CONSORCIO INCIBER.**
Tipo de Evaluación	EVALUACION TECNICA PRELIMINAR

Servicios de monitoreo y respuesta a incidentes cibernéticos

Cantidad	Especificaciones Técnicas	Propuesta	Comentario
1	Monitoreo en tiempo real de la infraestructura crítica del Poder Judicial.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 131.
	Análisis diario de bitácoras y comportamientos anómalos.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 131.
	Gestión de incidentes cibernéticos contemplando el primer y segundo nivel de soporte.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 131.
	Servicios de Inteligencia de Amenazas y Cacería de Amenazas (Threat Hunting).	Cumple	Cumple satisfactoriamente. Ver descripción en la página 131.
	La siguiente infraestructura debe ser monitoreada: a) 10 servicios web publicados en internet. b) 100 dispositivos alojados en una infraestructura de nube híbrida. c) Nombres de dominios adquiridos parecidos. d) Certificados digitales adquiridos parecidos. e) Correos fraudulentos haciéndose pasar por la institución. f) Robo de credenciales. g) Búsqueda de sitios falsos parecidos a los sitios del Poder Judicial. h) Fuga de datos en la Deep Web.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 132.
	Los siguientes casos de uso deben ser incluidos dentro del alcance del monitoreo: a) Creación, eliminación y modificación de objetos en el Directorio Activo. b) Delegación de permisos en el Active Directory. c) Usuarios agregados o removidos de grupos de seguridad / distribución. d) Cambios realizados en las políticas de grupo (GPO). e) Actividades relacionadas con inicios de sesión sospechosos. f) Seguimiento a cuentas privilegiadas. g) Infección de malware. h) Navegación y comunicaciones maliciosas. i) Ataques detectados en IPS.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 132.
	Tomar en consideración que el Poder Judicial cuenta con su propia infraestructura SIEM, Directorio Activo, antivirus, cifrado y cortafuegos.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 132.
	Servicios de asesoría y apoyo en la contención de riesgos identificados.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 132.
	Apoyo técnico remoto y/o presencial ante incidencias de seguridad que lo ameriten	Cumple	Cumple satisfactoriamente. Ver descripción en la página 132.
	El Poder Judicial debe tener acceso a los tableros (dashboards) en tiempo real de cada fuente de información monitoreada.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 132.
	Reportes de incidencias y postura de seguridad de los servicios críticos con periodicidad mensual y en demanda. También se deben generar reportes posteriores a una falla o incidente crítico de ciberseguridad.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 132.
	Reportes de cumplimiento con normativas de la familia ISO 27000.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 133.
	Suscripción del servicio de SOC 24/7 por un (1) año.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 133.
	Se debe contemplar la capacitación necesaria para 10 especialistas técnicos del Poder Judicial.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 133.

Otros requerimientos

No.	Descripción de Otros Requerimientos	Propuesta	Comentario
1	Cronograma de implementación.	Cumple	Ver detalles en Oferta Técnica, página 175, provisto por el oferente.
2	Documentación emitida por el representante local donde se especifiquen los tiempos de respuesta (SLA) de acuerdo a la criticidad de cada incidente de seguridad.	Cumple	Ver detalles en Oferta Técnica, página 187, provisto por el oferente.

FORMULARIO DE EVALUACIÓN DE PROPUESTA TÉCNICA
CONSEJO DEL PODER JUDICIAL

3	Incluir dentro de su propuesta técnica documentos de referencia de al menos tres (3) empresas o instituciones de más de 7,500 usuarios cuya infraestructura crítica esté siendo monitoreada a través de sus servicios de SOC.	No Cumple	No se evidencian las empresas o instituciones de mas de 7,500 usuarios. Por favor aclarar.
4	Incluir dentro de su propuesta certificaciones de cumplimiento en materia de seguridad de la información.	Cumple	Ver detalles en Oferta Técnica, página 167, provisto por el oferente.

FIN MATRIZ DE EVALUACIÓN TÉCNICA

FORMULARIO DE EVALUACIÓN DE PROPUESTA TÉCNICA
CONSEJO DEL PODER JUDICIAL

FORMULARIO DE EVALUACIÓN PROPUESTA TÉCNICA	
Nombre del Proceso	CONTRATACIÓN DE LOS SERVICIOS DE MONITOREO Y RESPUESTA A INCIDENTES CIBERNÉTICOS
Referencia del Proceso	**CP-CPJ-BS-12-2022**
Fecha de Evaluación	06 DE SEPTIEMBRE DE 2022
Oferente	**NETREADY RD, SRL.**
Tipo de Evaluación	EVALUACION TECNICA PRELIMINAR

Servicios de monitoreo y respuesta a incidentes cibernéticos

Cantidad	Especificaciones Técnicas	Propuesta	Comentario
1	Monitoreo en tiempo real de la infraestructura crítica del Poder Judicial.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 47.
	Análisis diario de bitácoras y comportamientos anómalos.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 47.
	Gestión de incidentes cibernéticos contemplando el primer y segundo nivel de soporte.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 47.
	Servicios de Inteligencia de Amenazas y Cacería de Amenazas (Threat Hunting).	Cumple	Cumple satisfactoriamente. Ver descripción en la página 47.
	La siguiente infraestructura debe ser monitoreada: a) 10 servicios web publicados en internet. b) 100 dispositivos alojados en una infraestructura de nube híbrida. c) Nombres de dominios adquiridos parecidos. d) Certificados digitales adquiridos parecidos. e) Correos fraudulentos haciéndose pasar por la institución. f) Robo de credenciales. g) Búsqueda de sitios falsos parecidos a los sitios del Poder Judicial. h) Fuga de datos en la Deep Web.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 47.
	Los siguientes casos de uso deben ser incluidos dentro del alcance del monitoreo: a) Creación, eliminación y modificación de objetos en el Directorio Activo. b) Delegación de permisos en el Active Directory. c) Usuarios agregados o removidos de grupos de seguridad / distribución. d) Cambios realizados en las políticas de grupo (GPO). e) Actividades relacionadas con inicios de sesión sospechosos. f) Seguimiento a cuentas privilegiadas. g) Infección de malware. h) Navegación y comunicaciones maliciosas. i) Ataques detectados en IPS.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 48.
	Tomar en consideración que el Poder Judicial cuenta con su propia infraestructura SIEM, Directorio Activo, antivirus, cifrado y cortafuegos.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 48.
	Servicios de asesoría y apoyo en la contención de riesgos identificados.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 48.
	Apoyo técnico remoto y/o presencial ante incidencias de seguridad que lo ameriten	Cumple	Cumple satisfactoriamente. Ver descripción en la página 48.
	El Poder Judicial debe tener acceso a los tableros (dashboards) en tiempo real de cada fuente de información monitoreada.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 48.
	Reportes de incidencias y postura de seguridad de los servicios críticos con periodicidad mensual y en demanda. También se deben generar reportes posteriores a una falla o incidente crítico de ciberseguridad.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 48.
	Reportes de cumplimiento con normativas de la familia ISO 27000.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 49.
	Suscripción del servicio de SOC 24/7 por un (1) año.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 49.
	Se debe contemplar la capacitación necesaria para 10 especialistas técnicos del Poder Judicial.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 49.

Otros requerimientos

No.	Descripción de Otros Requerimientos	Propuesta	Comentario
1	Cronograma de implementación.	Cumple	Ver detalles en Oferta Técnica, página 98, provisto por el oferente.
2	Documentación emitida por el representante local donde se especifiquen los tiempos de respuesta (SLA) de acuerdo a la criticidad de cada incidente de seguridad.	Cumple	Ver detalles en Oferta Técnica, página 78, provisto por el oferente.
3	Incluir dentro de su propuesta técnica documentos de referencia de al menos tres (3) empresas o instituciones de más de 7,500 usuarios cuya infraestructura crítica esté siendo monitoreada a través de sus servicios de SOC.	Cumple	Ver detalles en Oferta Técnica, página 19, provisto por el oferente.

FORMULARIO DE EVALUACIÓN DE PROPUESTA TÉCNICA
CONSEJO DEL PODER JUDICIAL

4	Incluir dentro de su propuesta certificaciones de cumplimiento en materia de seguridad de la información.	Cumple	Ver detalles en Oferta Técnica, página 111, provisto por el oferente.

FIN MATRIZ DE EVALUACIÓN TÉCNICA

FORMULARIO DE EVALUACIÓN DE PROPUESTA TÉCNICA
CONSEJO DEL PODER JUDICIAL

FORMULARIO DE EVALUACIÓN PROPUESTA TÉCNICA	
Nombre del Proceso	CONTRATACIÓN DE LOS SERVICIOS DE MONITOREO Y RESPUESTA A INCIDENTES CIBERNÉTICOS
Referencia del Proceso	**CP-CPJ-BS-12-2022**
Fecha de Evaluación	06 DE SEPTIEMBRE DE 2022
Oferente	**NAP DEL CARIBE, INC.**
Tipo de Evaluación	EVALUACION TECNICA PRELIMINAR

Servicios de monitoreo y respuesta a incidentes cibernéticos

Cantidad	Especificaciones Técnicas	Propuesta	Comentario
1	Monitoreo en tiempo real de la infraestructura crítica del Poder Judicial.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 36.
	Análisis diario de bitácoras y comportamientos anómalos.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 36.
	Gestión de incidentes cibernéticos contemplando el primer y segundo nivel de soporte.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 36.
	Servicios de Inteligencia de Amenazas y Cacería de Amenazas (Threat Hunting).	Cumple	Cumple satisfactoriamente. Ver descripción en la página 36.
	La siguiente infraestructura debe ser monitoreada: a) 10 servicios web publicados en internet. b) 100 dispositivos alojados en una infraestructura de nube híbrida. c) Nombres de dominios adquiridos parecidos. d) Certificados digitales adquiridos parecidos. e) Correos fraudulentos haciéndose pasar por la institución. f) Robo de credenciales. g) Búsqueda de sitios falsos parecidos a los sitios del Poder Judicial. h) Fuga de datos en la Deep Web.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 36, 37 y 38.
	Los siguientes casos de uso deben ser incluidos dentro del alcance del monitoreo: a) Creación, eliminación y modificación de objetos en el Directorio Activo. b) Delegación de permisos en el Active Directory. c) Usuarios agregados o removidos de grupos de seguridad / distribución. d) Cambios realizados en las políticas de grupo (GPO). e) Actividades relacionadas con inicios de sesión sospechosos. f) Seguimiento a cuentas privilegiadas. g) Infección de malware. h) Navegación y comunicaciones maliciosas. i) Ataques detectados en IPS.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 46.
	Tomar en consideración que el Poder Judicial cuenta con su propia infraestructura SIEM, Directorio Activo, antivirus, cifrado y cortafuegos.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 55.
	Servicios de asesoría y apoyo en la contención de riesgos identificados.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 36.
	Apoyo técnico remoto y/o presencial ante incidencias de seguridad que lo ameriten	Cumple	Cumple satisfactoriamente. Ver descripción en la página 36.
	El Poder Judicial debe tener acceso a los tableros (dashboards) en tiempo real de cada fuente de información monitoreada.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 60.
	Reportes de incidencias y postura de seguridad de los servicios críticos con periodicidad mensual y en demanda. También se deben generar reportes posteriores a una falla o incidente crítico de ciberseguridad.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 36.
	Reportes de cumplimiento con normativas de la familia ISO 27000.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 41.
	Suscripción del servicio de SOC 24/7 por un (1) año.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 36.
	Se debe contemplar la capacitación necesaria para 10 especialistas técnicos del Poder Judicial.	Cumple	Cumple satisfactoriamente. Ver descripción en la página 36.

Otros requerimientos

No.	Descripción de Otros Requerimientos	Propuesta	Comentario
1	Cronograma de implementación.	Cumple	Ver detalles en Oferta Técnica, página 71, provisto por el oferente.
2	Documentación emitida por el representante local donde se especifiquen los tiempos de respuesta (SLA) de acuerdo a la criticidad de cada incidente de seguridad.	Cumple	Ver detalles en Oferta Técnica, página 41, provisto por el oferente.

FORMULARIO DE EVALUACIÓN DE PROPUESTA TÉCNICA
CONSEJO DEL PODER JUDICIAL

3	Incluir dentro de su propuesta técnica documentos de referencia de al menos tres (3) empresas o instituciones de más de 7,500 usuarios cuya infraestructura crítica esté siendo monitoreada a través de sus servicios de SOC.	No Cumple	No se evidencian las empresas o instituciones de mas de 7,500 usuarios. Por favor aclarar.
4	Incluir dentro de su propuesta certificaciones de cumplimiento en materia de seguridad de la información.	Cumple	Ver detalles en Oferta Técnica, página 64, provisto por el oferente.

Elaborado por

Luis Joel Mejia
Analista de Continuidad
Consejo del Poder Judicial

Adderli De la Rosa
Coordinador de Seguridad de Infraestructura
Consejo del Poder Judicial

Emmanuel Tejada
Gerente de Seguridad de la Informacion
Consejo del Poder Judicial

Revisado por

Welvis Beltran
Director TIC
Consejo del poder Judicial

FIN MATRIZ DE EVALUACIÓN TÉCNICA