FORMULARIO RANSOMWARE

Los cuadros de respuesta sombreados con este color requieren una selección individual. Seleccione la opción de respuesta que describe mejor al solicitante.
Los cuadros de respuesta sombreados con este color representan preguntas en las que se pueden seleccionar varias respuestas. Tenga en cuenta que estas preguntas también

1	Con respecto a los esfuerzos del Solicitante para mitigar la suplantación de identidad ("Phishing"), seleccione todas las que correspondan		
	El Solicitante proporciona capacitación y concienciación sobre la seguridad cibernética a los empleados al menos una vez al año.	SI	
	El Solicitante utiliza ataques de phishing simulados para probar la conciencia de seguridad cibernética de los empleados al menos una vez al año.	SI	
	Cuando el Solicitante está realizando ataques de phishing simulados, la tasa de éxito fue inferior al 15% en la última prueba (menos del 15% de los empleados dieron click al phishing exitosamente).	SI	
	El Solicitante "etiqueta" o marca los correos electrónicos de fuera de la organización.	SI	
	El Solicitante tiene un proceso para reportar correos electrónicos sospechosos a un equipo de seguridad interno para que los investigue.	SI	
	Ninguna de las anteriores		
	Comentarios adicionales sobre los esfuerzos de la compañía para mitigar el phishing / *Additional Commentary on efforts to mitigate phishing:*	SI	Campáñas y correos electrónicos para concienciación, monitorización de vigilancia digital sobre phishing, validación del correo eléctrónico sobre mecanismos de verificación, pruebas técnicas de seguridad, búsquedas en Deepweb, monitorización de noticias sobre phishing y vectores de ataque, gestión de desmonte de sitios web con phishing, etc.
	Campáñas y correos electrónicos para concienciación, monitorización de vigilancia digital sobre phishing, validación del correo eléctrónico sobre mecanismos de verificación, pruebas técnicas de seguridad, búsquedas en Deepweb, monitorización de noticias sobre phishing y vectores de ataque, gestión de desmonte de sitios web con phishing, etc.		
2	¿El Solicitante tiene un proceso documentado para responder a las campañas de phishing (ya sea que estén dirigidas específicamente al solicitante o no)?		
	Sí / yes		
	No	X	
	Si la respuesta es "Sí", describa los pasos principales para responder: Norma interna de seguridad informática		
3	Con respecto a los esfuerzos del **Solicitante** para bloquear sitios web y/o correo electrónico potencialmente maliciosos, seleccione todo lo que corresponda:		
	El **Solicitante** utiliza una solución de filtrado de correo electrónico que bloquea los archivos adjuntos maliciosos conocidos y los tipos de archivos sospechosos, incluidos los ejecutables. *Applicant uses an e-mail filtering solution which blocks known malicious attachments and suspicious file types, including executables.*	SI	
	El **Solicitante** utiliza una solución de filtrado de correo electrónico que bloquea los mensajes sospechosos en función de su contenido o los atributos del remitente. *Applicant uses an e-mail filtering solution which blocks suspicious messages based on their content or attributes of the sender.*	SI	
	El **Solicitante** utiliza una solución de filtrado web que evita que los empleados visiten páginas web sospechosas o maliciosas.	SI	
	El **Solicitante** bloquea dominios no categorizados y recién registrados mediante servidores proxy web o filtros DNS.	SI	
	El **Solicitante** utiliza una solución de filtrado web que bloquea las descargas sospechosas o maliciosas conocidas, incluidos los ejecutables. *Applicant uses a web-filtering solution which blocks known malicious or suspicious downloads, including executables.*	SI	
	La solución de filtrado de correo electrónico del **Solicitante** tiene la capacidad de ejecutar archivos adjuntos sospechosos en una zona de pruebas o entorno aislado *Applicant's e-mail filtering solution has the capability to run suspicious attachments in a sandbox.*	SI	
	Las capacidades de filtrado web del **Solicitante** son efectivas en todos los activos corporativos, incluso si el activo corporativo no está en una red corporativa (por ejemplo, los activos están configurados para utilizar filtros web basados en la nube o requieren una conexión VPN para navegar por Internet). *Applicant's web filtering capabilities are effective on all corporate assets, even if the corporate asset is not on a corporate network (e.g. assets are configured to utilize cloud-*	SI	
	Ninguna de las anteriores / *None of the above.*		
	Comentarios adicionales sobre los esfuerzos para bloquear sitios web y/o correo electrónico maliciosos: *Additional commentary on efforts to block malicious websites and/or email:*	SI	Se tienen herramientas para bloquear el acceso a ciertos sitios WEB que intenten acceder por parte de los empleados y para bloquear el correo lectrónico malicioso.
	Se tienen herramientas para bloquear el acceso a ciertos sitios WEB que intenten acceder por parte de los empleados y para bloquear el correo lectrónico malicioso.		
4	Con respecto a la autenticación para los empleados que acceden de forma remota a la red corporativa y cualquier servicio basado en la nube donde puedan residir datos confidenciales (incluido el acceso al VPN , correo electrónico y CRM basados en la nube; juntos "**acceso remoto a los recursos corporativos**"), seleccione la descripción que mejor refleje la postura del Solicitante: (Como se usa en este documento, "autenticación multifactor" significa autenticación que utiliza al menos dos tipos diferentes de posibles factores de autenticación (algo que usted sabe, algo que tiene y algo que eres); el solicitante puede proporcionar una explicación más detallada a continuación) *With respect to authentication for employees who are remotely accessing the corporate network and any cloud-based services where sensitive data may reside (including VPN*		
	El acceso remoto a los recursos corporativos requiere un nombre de usuario y una contraseña válidas (autenticación de factor único).		
	La autenticación multifactor está implementada para algunos tipos de acceso remoto a los recursos corporativos, pero no para todos.		
	La política exige la autenticación multifactor para todos los accesos remotos a los recursos corporativos; todas las excepciones a la política están documentadas.	X	
	El **Solicitante** no proporciona acceso remoto a los empleados. / *Applicant does not provide remote access to employees.*		
	Comentarios adicional sobre autenticación para empleados: / *Additional commentary on authentication for employees:*		
5	Con respecto a la autenticación para contratistas y proveedores independientes que acceden remotamente a la red corporativa y cualquier servicio basado en la nube donde los datos confidenciales pueden residir (incluido el acceso VPN y el correo electrónico y CRM basados en la nube; juntos "acceso remoto a los recursos corporativos")), seleccione la descripción que mejor refleje la postura del solicitante: (El solicitante puede proporcionar más explicaciones a continuación).		
	El acceso remoto a los recursos corporativos requiere un nombre de usuario y una contraseña válidas (autenticación de factor único).		
	La autenticación multifactor está implementada para algunos tipos de acceso remoto a los recursos corporativos, pero no para todos.		
	La política exige la autenticación multifactor para todos los accesos remotos a los recursos corporativos; todas las excepciones a la política están documentadas.	X	
	El **Solicitante** no proporciona acceso remoto a los contratistas y proveedores independientes / *Applicant does not provide remote access to independent contractors/vendors.*		
	Comentarios adicional sobre autenticación para contratistas y proveedores independientes / *Additional commentary on authentication for independent contractors/vendors:*		
6	¿La implementación de autenticación multifactor del solicitante también cumple los criterios de que el compromiso de un solo dispositivo sólo comprometerá un único autenticador? (A modo de ejemplo: cuando la autenticación requiere una contraseña (conocimiento) y un token (posesión), esto no cumpliría los criterios anteriores si el token para probar la posesión es mantener en un dispositivo la contraseña que también se introduce, exponiendo ambos si el dispositivo está en peligro) *Does the Applicant's multifactor authentication implementation also meet the criteria that the compromise of any single device will only compromise a single authenticator? (For illustration: where authentication requires a password (knowledge) and a token (possession), this would not meet the criteria above if the token to prove possession is kept on a device the password is also entered into, exposing both if the device is compromised)*		
	No aplicable (el **Solicitante** no utiliza la autenticación multifactor) / *Not Applicable (Applicant does not use multi-factor authentication)*		
	No; La implementación multifactor del **Solicitante** no cumple los criterios anteriores. / *No; Applicant's multi-factor implementation does not meet the above criteria.*		
	Sí; la implementación multifactor del solicitante cumple con los criterios anteriores. / *Yes; the Applicant's multi-factor implementation meets the above criteria.*	X	
	Comentarios adicionales sobre la implementación de la autenticación multifactor: / *Additional commentary on Multi-factor authentication implementation:*		
7	Con respecto a la seguridad en los endpoints de estaciones de trabajo (computadoras y laptops), seleccione todas las que correspondan:		
	La política del **Solicitante** es que todas las estaciones de trabajo tienen antivirus con capacidades heurísticas.	SI	
	El **Solicitante** utiliza herramientas de seguridad de endpoints con capacidades de detección del comportamiento y mitigación de vulnerabilidades.	SI	
	El **Solicitante** tiene un grupo interno que supervisa la salida de las herramientas de seguridad en los endpoints e investiga cualquier anomalía.	SI	
	Ninguna de las anteriores / *None of the above.*		
	Comentario adicional sobre las capacidades de seguridad de los endpoints: / *Additional commentary on endpoint security capabilities:*		
8	Con respecto a la supervisión de las herramientas de salida de seguridad, seleccione la descripción que mejor refleje las capacidades del solicitante: (El solicitante puede proporcionar una explicación más detallada a continuación) *With respect to monitoring the output of security tools, select the description which best reflects the Applicant's capabilities: (The Applicant can provide further explanation below)*		
	El **Solicitante** no tiene personal dedicado a supervisar las operaciones de seguridad **(un "Security Operations Center")**.		
	El **Solicitante** tiene un centro de operaciones de seguridad **("Security Operations Center")**, pero no es 24/7 (puede ser interno o externo).		
	El **Solicitante** tiene una supervisión 24/7 de las operaciones de seguridad mediante un tercero (como un proveedor de servicios de seguridad).	X	

	El **Solicitante** tiene monitoreo 24/7 de las operaciones de seguridad internamente.	
	Comentarios adicionales sobre la supervisión de la seguridad: / *Additional commentary on security monitoring:*	
9	¿Cuál es el tiempo medio del solicitante para evaluar y contener incidentes de seguridad de estaciones de trabajo? (El **Solicitante** puede proporcionar más explicaciones a continuación) *What is the Applicant's average time to triage and contain security incidents of workstations year to date? (The Applicant can provide further explanation below)*	
	El **Solicitante** no rastrea esta métrica/No sabe / *Applicant does not track this metric/Do not know*	
	<30 minutos/Minutes	
	30 minutos/minutes - 2 horas/hours	X
	2-8 horas/hours	
	>8 horas/hours	
	Comentario adicional sobre el tiempo promedio para corregir: / *Additional commentary on average time to remediate:*	
10	Con respecto a los controles de acceso para la estación de trabajo de cada usuario, seleccione la descripción que mejor refleje la postura del **Solicitante**:	
	Ningún empleado está en el grupo de administradores ni tiene acceso de administrador local a sus estaciones de trabajo.	X
	La política del **Solicitante** es que los empleados de forma predeterminada no están en el grupo de administradores y no tienen acceso de administrador local; todas las	
	Algunos de los empleados del **Solicitante** están en el grupo de administradores o son administradores locales. *Some of Applicant's employees are in the Administrators' group or are local admins.*	
	No sabe / *Do not know.*	
	Comentarios adicionales sobre los controles de acceso para estaciones de trabajo: / *Additional commentary on access controls for workstations:*	
11	Con respecto a la protección de credenciales privilegiadas, seleccione todas las que correspondan con la postura del **Solicitante**:	
	Los administradores del sistema del solicitante tienen una credencial única y privilegiada para las tareas administrativas (independientemente de sus credenciales de usuario de acceso diario, email, etc.). *System administrators at the Applicant have a unique, privileged credential for administrative tasks (separate from their user credentials for everyday access, email, etc.).*	SI
	Las cuentas con privilegios (incluidos los administradores de dominio) requieren autenticación multifactor.	SI
	Las cuentas privilegiadas se guardan en un lugar seguro con contraseña que requieren que el usuario "revise" la credencial (que luego se rota).	SI
	Hay un registro de todo el uso de la cuenta con privilegios durante al menos los últimos treinta días.	SI
	Las estaciones de trabajo de acceso con privilegios (estaciones de trabajo que no tienen acceso a Internet o correo electrónico) se utilizan para la administración de sistemas críticos (incluidos los servidores de autenticación/ Controladores de dominio). *Privileged Access Workstations (workstations that do not have access to internet or e-mail) are used for the administration of critical systems (including authentication servers/*	SI
	Ninguna de las anteriores / *None of the above.*	
	Comentarios adicionales sobre la protección de credenciales con privilegios: / *Additional commentary on protecting privileged credentials:*	
12	Indique el uso de Microsoft Active Directory por parte del solicitante (en todos los dominios o "forests"):	
	El **Solicitante** no utiliza Microsoft Active Directory (indicar a la derecha)	SI
	Número de cuentas de usuario en el grupo Administradores de dominio (incluya cuentas de servicio , si las hay, en este total):	4
	Número de cuentas de servicio en el grupo Administradores de dominio:	6
	Comentario adicional sobre el número de administradores de dominio: / *Additional commentary on the number of Domain Administrators:*	
13	¿Cuántos usuarios tienen cuentas privilegiadas persistentes para endpoints (servidores y estaciones de trabajo)?	
	Introduzca un número entero: / *Please enter an integer:*	10
	Comentario adicional sobre el número de cuentas con privilegios: / *Additional commentary on the number of privileged accounts:*	
14	Con respecto a la seguridad de los sistemas externos, seleccione todo lo que corresponda a la postura del **Solicitante**:	
	El **Solicitante** realiza una prueba de penetración al menos una vez al año para evaluar la seguridad de sus sistemas externos *Applicant conducts a penetration test at least annually to assess the security of its externally facing systems.*	SI
	El **Solicitante** tiene un firewall de aplicaciones web ("Web Application Firewall" - WAF) frente a todas las aplicaciones externas y está en modo de bloqueo. *Applicant has a Web Application Firewall (WAF) in front of all externally facing applications, and it is in blocking mode.*	SI
	El **Solicitante** utiliza un servicio externo para monitorear su superficie de ataque (sistemas externos/orientados a Internet). *Applicant uses an external service to monitor its attack surface (external/internet facing systems).*	SI
	Ninguna de las anteriores / *None of the above.*	
15	¿Cuál es el tiempo objetivo del **Solicitante** para implementar parches "críticos", de alta prioridad, (según lo determinen los estándares del solicitante para cuándo deben implementarse los parches)? *What is the Applicant's target time to deploy 'critical' – the highest priority – patches (as determined by the Applicant's standards for when patches must be deployed)?*	
	No hay ninguna directiva definida para cuando se deben implementar revisiones. / *There is no defined policy for when patches must be deployed.*	
	Dentro de 24 horas. / *Within 24 hours.*	SI
	24-72 horas/hours	
	3-7 días/days	
	> 7 días/days	
	Comentario adicional sobre los tiempos de destino para la aplicación de parches: / *Additional commentary on target times for patching:*	
16	¿Cuál es el % de cumplimiento de los propios estándares del **Solicitante** al año para la implementación de parches críticos?	
	Applicant does not track this metric/Do not know / *Applicant does not track this metric/Do not know*	
	>95%	SI
	90-95%	
	80-90%	
	<80%	
	Comentarios adicionales sobre el cumplimiento de los parches: / *Additional commentary on patching compliance:*	
17	Con respecto a las capacidades de supervisión de la red del **Solicitante**, seleccione todas las que correspondan:	
	El **Solicitante** utiliza una herramienta de monitoreo de eventos e información de seguridad (SIEM) para correlacionar la salida de múltiples herramientas de seguridad.} *Applicant uses a security information and event monitoring (SIEM) tool to correlate the output of multiple security tools.*	SI
	El **Solicitante** monitorea el tráfico de la red en busca de transferencias de datos anómalas y potencialmente sospechosas.	SI
	El **Solicitante** supervisa los problemas de rendimiento y capacidad de almacenamiento (como un uso elevado de memoria o procesador, o falta de espacio libre en el disco).	SI
	El **Solicitante** tiene herramientas para monitorear la pérdida de datos (DLP) y están en modo de bloqueo. *Applicant has tools to monitor for data loss (DLP) and they are in blocking mode.*	SI
	Ninguna de las anteriores / None of the above.	
	Comentarios adicionales sobre la supervisión de la red: / *Additional commentary on network monitoring:*	
18	Con respecto a limitar el movimiento lateral, seleccione todo lo que se aplique a la postura del **Solicitante**:	
	El **Solicitante** ha segmentado la red por geografía (por ejemplo, se deniega el tráfico entre oficinas en diferentes ubicaciones a menos que sea necesario para apoyar un requisito empresarial específico). *Applicant has segmented the network by geography (e.g. traffic between offices in different locations is denied unless required to support a specific business requirement).*	SI
	El **Solicitante** ha segmentado la red por función empresarial (por ejemplo, se prohibe el tráfico entre activos que soportan diferentes funciones (Recursos Humanos y Finanzas, por ejemplo) a menos que sea necesario para apoyar un requisito empresarial específico). *Applicant has segmented the network by business function (e.g. traffic between asset supporting different functions – HR and Finance for example – is denied unless required to support a specific business requirement).*	SI
	El **Solicitante** ha implementado reglas de firewall de host que impiden el uso de RDP para iniciar sesión en estaciones de trabajo.	SI
	El **Solicitante** ha configurado todas las cuentas de servicio para denegar los inicios de sesión interactivos.	SI
	Ninguna de las anteriores / *none of the above*	
	Comentario adicional sobre la segmentación: / *Additional commentary on segmentation:*	

19	Introduzca la fecha del último ejercicio ransomware del **Solicitante**; marque la casilla si no se ha llevado a cabo ninguno.	
	Fecha/date:	SI
	No se ha realizado ningún ejercicio ransomware. / *No ransomware exercise has been conducted.*	15/08/2026
20	¿Tiene el solicitante un plan documentado para responder al ransomware de un proveedor/proveedor o cliente tercero? En caso afirmativo, indique los pasos principales. *Does the Applicant have a documented plan to respond to ransomware of a 3rd party provider/vendor or customer? If yes, please indicate principle steps.*	
	No (Le cayó Ransomware a un proveedor y no nos puede despachar)	X
	Sí/yes	
	Principales pasos realizado por el tercero: / *3rd party ransomware response principle steps:*	
21	Con respecto a la verificación de la eficacia de los controles de seguridad, seleccione todo lo que se aplica al **Solicitante**:	
	El **solicitante** utiliza el software de simulación de infracciones y ataques (BAS) para verificar la eficacia de los controles de seguridad.	
	El **Solicitante** tiene un "red team" interno que prueba los controles de seguridad y la respuesta de los mismos.	SI
	El **Solicitante** ha contratado a una parte externa para simular actores de amenazas y probar controles de seguridad en el último año.	SI
	Ninguna de las anteriores / *none of the above*	
	Comentario adicional sobre la verificación de los controles: / *Additional commentary on controls verification:*	
22	Con respecto a las capacidades de recuperación ante desastres, seleccione todas las que se aplican al **Solicitante**:	
	Existe un proceso para crear copias de seguridad, pero es indocumentado y/o ad hoc	SI
	El **Solicitante** tiene una política de recuperación ante desastres documentada, que incluye estándares para copias de seguridad basadas en la criticidad de la información. *Applicant has a documented Disaster Recovery Policy, including standards for backups based on information criticality.*	SI
	Al menos dos veces al año, el **Solicitante** pone a prueba su capacidad para restaurar diferentes sistemas y datos críticos de manera oportuna a partir de sus copias de seguridad. *At least twice a year, Applicant tests its ability to restore different critical systems and data in a timely fashion from its backups.*	SI
	Ninguna de las anteriores / *none of the above*	
23	¿Cuál es el tiempo de recuperación objetivo (RTO) del **Solicitante** para los sistemas críticos?	
	El **Solicitante** no tiene un RTO/No sabe	
	< 4 horas/hours.	
	4-24 horas/hours..	SI
	1 to 2 días/days.	
	2-7 días/days.	
24	Con respecto a las capacidades de las copias de seguridad, seleccione todas las que se aplican al **Solicitante**	
	La estrategia de copia de seguridad del **Solicitante** incluye copias de seguridad sin conexión (se pueden almacenar en el sitio)	SI
	La estrategia de copia de seguridad del **solicitante** incluye copias de seguridad sin conexión almacenadas fuera del sitio	SI
	Solo se puede acceder a las copias de seguridad del solicitante a través de un mecanismo de autenticación fuera de nuestro Active Directory corporativo.	
	Comentarios adicionales sobre las capacidades de copia de seguridad: / *Additional commentary on backup capabilities:*	
25	¿El **Solicitante cuenta con** alguna política que todos los dispositivos portátiles utilizan cifrado de disco completo?	
	Si/yes	X
	No	
	Comentarios Adicionales: / *Additional Comments:*	

ESTE CUESTIONARIO COMPLEMENTARIO SE INCORPORA Y FORMA PARTE DE CUALQUIER SOLICITUD DE COBERTURA DE RIESGOS CIBERNÉTICOS POR PARTE DEL SOLICITANTE.

Empresa Solicitante:
Applicant

Firma:



Título:
Gerente Administrativa y Financiera

Fecha:

28 de septiembre de 2026