

El presente formulario es una recopilación de diferentes preguntas que requieren los mercados sobre el tema Ransomware, es necesario su diligenciamiento para poder tener acceso a todos los mercados. Es importante tener en cuenta que en el proceso de cotización pueden surgir preguntas adicionales específicas.

Beqley

Email Security

7A ¿Utilizan Office 365 en su compañía?
Do you use Office 365 in your organisation? Yes No

7B En caso afirmativo: ¿Utilizan Office 365 Advanced Threat Protection añadido?
If Yes: Do you use the o365 Advanced Threat Protection add-on? Yes No

Internal Security

12 ¿Qué porcentaje de la empresa cubren los escáneres de vulnerabilidades que tienen programados?
What % of the enterprise is covered by your scheduled vulnerability scans? 600 OBJETIVOS

14 ¿Tienen algún software que esté terminando su vida útil o sistemas legacy, en caso afirmativo están segregados del resto de la red?
Do you have any end of life or end of support software, if yes: is it segregated from the rest of the network? Yes No Partial N/A

17 ¿Utilizan una aplicación de aislamiento y tecnología de contención en los usuarios finales?
Do you use an endpoint application isolation and containment technology?
Escala una / Choose one:
 Menlo Security Isolation Platform
 Authentic8 Silo
 Symantec Web Security Service (WSS) - Web Isolation
 CylanceProtect
 Puffin Secure Browser
 Apoxy
 Bitdefender Browser Isolation
 Cyliso Remote Browsing
 Cyberinc Isla
 Passages by Ntrepid
 WEBGAP Remote Browser
 Curose Internet Isolation
 Cyberwall
 Garrison SAVI
 Light Point Web
 Morphisec Endpoint Threat Prevention - Browser Based Attacks
 Randed AGU
 Utilizamos un producto que no esta en la lista / We use a product not on above list
 No hemos implementado tal producto / We have not deployed such a product
 Otro / Other (Favor especificar / please specify): Utilizamos un producto que no esta en la lista / We use a product not on above list (SOPHOS)

19 ¿Pueden los usuarios utilizar de MS Office Macro para los documentos habilitados por defecto?
Can users run MS Office Macro enabled documents on their system by default? Yes No Partial N/A

20 ¿Proveen a los usuarios de un software que gestione las contraseñas?
Do you provide your users with a password manager software? Yes No

Back-up and Recovery Policies

23 ¿Los Back-ups (copias de seguridad) están sujetos a las siguientes medidas?
Are backups subject to the following measures?
 Seleccione las que apliquen / Select all that apply:
 Encriptación / Encryption Segmentación / Segmentation Escaneo de Virus-malware / Virus-malware scanning Credenciales de respaldo únicas almacenadas por separado de otras credenciales de usuario / Unique backup credentials stored separately from other user credentials

27 ¿Tienen la capacidad de comprobar la integridad de los back-ups (copias de seguridad) antes de su restauración para confirmar que están libres de malware?
Are you able to test the integrity of back-ups prior to restoration to be confident it is free from malware? Yes No Partial N/A

Axis

1 ¿Emplea el solicitante alguna solución de detección y prevención de intrusiones?
Does the applicant employ any intrusion detection and prevention solution? Yes No

2 ¿El solicitante tiene implementada la autenticación multifactor?
Does the applicant has Multi-factor authentication implemented Yes No

3 ¿Se requiere autenticación multifactor para acceder a información crítica, dispositivos personales e información y aplicaciones no críticas?
Is Multi factor authentication required for access to critical information, personal devices and noncritical information and applications? Yes No

4 ¿El solicitante emplea SPF, DKIM o DMARC?
Does the applicant employ SPF, DKIM, or DMARC? Yes No Pendiente DMARC

5 ¿Está habilitado el Protocolo de escritorio remoto (RDP)?
Is Remote Desktop Protocol (RDP) enabled?
 a. En caso afirmativo seleccione una / if yes select one:
 Autenticación de nivel de red habilitada / Network level authentication enabled ; Acceso solo por VPN / VPN access only ; Autenticación multifactor para acceso / Multi factor authentication for access ; Protocolo de escritorio remoto / RDP honeypot(s) ; **Alguna otra, favor especificar / any other, please specify?** Cyberark- y acceso RDP de usuarios para terminal

6 ¿El solicitante realiza copias de seguridad periódicas de los datos?
Does the applicant conduct regular back up of data? Yes No

7 ¿Con qué frecuencia se realiza una copia de seguridad de la información crítica?
How frequently is Critical Information backed up? Diaría

8 ¿El solicitante utiliza cintas de respaldo físicas?
Does the applicant utilize physical backup tapes Yes No

9 ¿Con qué frecuencia se realizan las copias de seguridad en el almacenamiento externo?
How frequently are backups made to offsite storage? QUINCENAL

10 En el caso de que la Información crítica, o los sistemas, aplicaciones o procesos críticos no estuvieran disponibles, ¿cuánto tiempo tomaría interrumpir materialmente el negocio del solicitante? A lo sumo:
In the event Critical Information, or critical systems, applications or processes became unavailable, how long would it take to materially interrupt the applicant's business? At most:
 < 1 hora/hours 1-8 horas/hours 8-12 horas/hours 12-24 horas/hours 24-48 horas/hours 1-8 HORAS

AIG

Los cuadros de respuesta sombreados con este color requieren una selección individual. Seleccione la opción de respuesta que describe mejor al solicitante.
Response boxes shaded this color require an individual selection, effectively, which response option best describes the Applicant.

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 especificarán "seleccione todo lo que corresponda".
Response boxes shaded this color represent questions in which you can select multiple answers. These questions will also specify "select all that apply".

1 Con respecto a los esfuerzos del Solicitante para mitigar la suplantación de identidad ("Phishing"), seleccione todas las que correspondan
With respect to the Applicant's efforts to mitigate phishing, select all that apply.

El Solicitante proporciona capacitación y concienciación sobre la seguridad cibernética a los empleados al menos una vez al año.
Applicant provides security awareness training to employees at least annually.

El Solicitante utiliza ataques de phishing simulados para probar la conciencia de seguridad cibernética de los empleados al menos una vez al año.
Applicant uses simulated phishing attacks to test employees' cybersecurity awareness at least annually.

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).
Where the Applicant is conducting simulated phishing attacks, the success ratio was less than 15% on the last test (less than 15% of employees were successfully phished).

<p>El Solicitante "etiqueta" o marca los correos electrónicos de fuera de la organización. <i>Applicant "tags" or otherwise marks e-mails from outside the organization.</i></p> <p>El Solicitante tiene un proceso para reportar correos electrónicos sospechosos a un equipo de seguridad interno para que los investigue. <i>Applicant has a process to report suspicious e-mails to an internal security team to investigate.</i></p> <p>Ninguna de las anteriores <i>None of the above.</i></p> <p>Comentarios adicionales sobre los esfuerzos de la compañía para mitigar el phishing / <i>Additional Commentary on efforts to mitigate phishing:</i></p> <p>Se efectúan seguimientos periódicos sobre la plataforma de office365 y sensibilizaciones por correo al personal</p>	<p>X</p> <p>X</p>
<p>2 ¿El Solicitante tiene un proceso documentado para responder a las campañas de phishing (ya sea que estén dirigidas específicamente al solicitante o no)? <i>Does the Applicant have a documented process to respond to phishing campaigns (whether targeted specifically at the Applicant or not)?</i></p> <p>Si / yes</p> <p>No</p> <p>Si la respuesta es "SI", describa los pasos principales para responder: <i>If "Yes," please describe the principal steps to respond:</i></p> <p>Detección: revisar síntomas y encabezados, validar direccionamiento del correo, revisar en plataforma correos enviados <i>Detection: identify credentials compromised and effect changes, identify systems affected, validate code malicious, block sources identified, identify propagation</i></p>	<p>X</p>
<p>3 Con respecto a los esfuerzos del Solicitante para bloquear sitios web y/o correo electrónico potencialmente maliciosos, seleccione todo lo que corresponda: <i>With respect to the Applicant's efforts to block potentially harmful websites and/or email, select all that apply:</i></p> <p>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. <i>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.</i> <i>Applicant uses an e-mail filtering solution which blocks suspicious messages based on their content or attributes of the sender.</i></p> <p>El Solicitante utiliza una solución de filtrado web que evita que los empleados visiten páginas web sospechosas o maliciosas. <i>Applicant uses a web filtering solution which stops employees from visiting known malicious or suspicious web pages.</i></p> <p>El Solicitante bloquea dominios no categorizados y recién registrados mediante servidores proxy web o filtros DNS. <i>Applicant uses block uncategorized and newly registered domains using web proxies or DNS filters.</i></p> <p>El Solicitante utiliza una solución de filtrado web que bloquea las descargas sospechosas o maliciosas conocidas, incluidos los ejecutables. <i>Applicant uses a web filtering solution which blocks known malicious or suspicious downloads, including executables.</i></p> <p>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 <i>Applicant's e-mail filtering solution has the capability to run suspicious attachments in a sandbox.</i></p> <p>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). <i>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-based web filters or require a VPN connection to browse the internet).</i></p> <p>Ninguna de las anteriores / <i>None of the above.</i></p> <p>Comentarios adicionales sobre los esfuerzos para bloquear sitios web y/o correo electrónico maliciosos: <i>Additional commentary on efforts to block malicious websites and/or email:</i></p> <p>Estamos finalizando implementación de SWG para teletrabajadores</p>	<p>X</p> <p>X</p> <p>X</p> <p>X</p> <p>X</p> <p>X</p> <p>X</p>
<p>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) <i>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 access, and cloud-based email and CRM; together "remote access to corporate resources"), select the description which best reflects the Applicant's posture: (As used herein, "multi-factor authentication" means authentication which uses at least two different types of the possible authentication factors (something you know, something you have, and something you are); the Applicant can provide further explanation below)</i></p> <p>El acceso remoto a los recursos corporativos requiere un nombre de usuario y una contraseña válidas (autenticación de factor único). <i>Remote access to corporate resources requires a valid username and password (single factor authentication).</i></p> <p>La autenticación multifactor está implementada para algunos tipos de acceso remoto a los recursos corporativos, pero no para todos. <i>Multi-factor authentication is in place for some types of remote access to corporate resources, but not all.</i></p> <p>La política exige la autenticación multifactor para todos los accesos remotos a los recursos corporativos; todas las excepciones a la política están documentadas. <i>Multi-factor authentication is required by policy for all remote access to corporate resources; all exceptions to the policy are documented.</i></p> <p>El Solicitante no proporciona acceso remoto a los empleados. / <i>Applicant does not provide remote access to employees.</i></p> <p>Comentarios adicional sobre autenticación para empleados: / <i>Additional commentary on authentication for employees:</i></p> <p>Uso de MFA para Office365, VPN y Salesforce</p>	<p>X</p>
<p>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: <i>(El solicitante puede proporcionar más explicaciones a continuación).</i> <i>With respect to authentication for independent contractors and vendors who are remotely accessing the corporate network and any cloud-based services where sensitive data may reside (including VPN access, and cloud-based email and CRM; together "remote access to corporate resources"), select the description which best reflects the Applicant's posture: (The Applicant can provide further explanation below):</i></p> <p>El acceso remoto a los recursos corporativos requiere un nombre de usuario y una contraseña válidas (autenticación de factor único). <i>Remote access to corporate resources requires a valid username and password (single factor authentication).</i></p> <p>La autenticación multifactor está implementada para algunos tipos de acceso remoto a los recursos corporativos, pero no para todos. <i>Multi-factor authentication is in place for some types of remote access to corporate resources, but not all.</i></p> <p>La política exige la autenticación multifactor para todos los accesos remotos a los recursos corporativos; todas las excepciones a la política están documentadas. <i>Multi-factor authentication is required by policy for all remote access to corporate resources; all exceptions to the policy are documented.</i></p> <p>El Solicitante no proporciona acceso remoto a los contratistas y proveedores independientes / <i>Applicant does not provide remote access to independent contractors/vendors.</i></p> <p>Comentarios adicional sobre autenticación para contratistas y proveedores independientes / <i>Additional commentary on authentication for independent contractors/vendors:</i></p> <p>Se maneja MFA para todo el personal externo a nivel de VPN y office365, a nivel interno se cuenta con UBA y monitoreo de aplicaciones sobre los usuarios que se conectan a la red.</p>	<p>X</p>
<p>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? <i>(A modo de ejemplo: cuando la autenticación requiere una contraseña (conocimiento) y un token (posesión), esto no cumplirá 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)</i> <i>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)</i></p> <p>No aplicable (el Solicitante no utiliza la autenticación multifactor) / <i>Not Applicable (Applicant does not use multi-factor authentication):</i> <input checked="" type="checkbox"/></p> <p>No; La implementación multifactor del Solicitante no cumple los criterios anteriores. / <i>No; Applicant's multi-factor implementation does not meet the above criteria.</i></p> <p>Si; la implementación multifactor del solicitante cumple con los criterios anteriores. / <i>Yes; the Applicant's multi-factor implementation meets the above criteria.</i></p> <p>Comentarios adicionales sobre la implementación de la autenticación multifactor: / <i>Additional commentary on Multi-factor authentication implementation:</i></p> <p>Se tienen varias opciones para el uso de los tokens por lo que no dependen de un solo dispositivo.</p>	<p>X</p>
<p>7 Con respecto a la seguridad en los endpoints de estaciones de trabajo (computadoras y laptops), seleccione todas las que correspondan: <i>With respect to the Applicant's endpoint security of workstations (desktops and laptops), select all that apply:</i></p> <p>La política del Solicitante es que todas las estaciones de trabajo tienen antivirus con capacidades heurísticas. <i>Applicant's policy is that all workstations have antivirus with heuristic capabilities.</i></p> <p>El Solicitante utiliza herramientas de seguridad de endpoints con capacidades de detección del comportamiento y mitigación de vulnerabilidades. <i>Applicant uses endpoint security tools with behavioral-detection and exploit mitigation capabilities.</i></p> <p>El Solicitante tiene un grupo interno que supervisa la salida de las herramientas de seguridad en los endpoints e investiga cualquier anomalía. <i>Applicant has an internal group which monitors the output of endpoint security tools and investigates any anomalies.</i></p> <p>Ninguna de las anteriores / <i>None of the above.</i></p> <p>Comentario adicional sobre las capacidades de seguridad de los endpoints: / <i>Additional commentary on endpoint security capabilities:</i></p>	<p>X</p> <p>X</p> <p>X</p>
<p>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) <i>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)</i></p> <p>El Solicitante no tiene personal dedicado a supervisar las operaciones de seguridad (un "Security Operations Center"). <i>Applicant does not have staff dedicated to monitoring security operations (a "Security Operations Center").</i></p> <p>El Solicitante tiene un centro de operaciones de seguridad ("Security Operations Center"), pero no es 24/7 (puede ser interno o externo). <i>Applicant has a Security Operations Center, but it's not 24/7 (can be internal or external).</i></p> <p>El Solicitante tiene una supervisión 24/7 de las operaciones de seguridad mediante un tercero (como un proveedor de servicios de seguridad). <i>Applicant has a 24/7 monitoring of security operations by a 3rd party (such as a Managed Security Services Provider).</i></p>	<p>X</p>

<p>El Solicitante tiene monitoreo 24/7 de las operaciones de seguridad internamente. <i>Applicant has 24/7 monitoring of security operations internally.</i></p> <p>Comentarios adicionales sobre la supervisión de la seguridad: / <i>Additional commentary on security monitoring:</i></p> <p>El servicio de SOC es operado por un representante con certificaciones internacionales SOC 2 y hace parte de FIRST</p>	
<p>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) <i>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)!</i></p> <p>El Solicitante no rastrea esta métrica/No sabe / <i>Applicant does not track this metric/Do not know</i></p> <p><30 minutos/Minutes 30 minutos/minutes - 2 horas/hours 2-8 horas/hours >8 horas/hours</p> <p>Comentario adicional sobre el tiempo promedio para corregir: / <i>Additional commentary on average time to remediate:</i></p> <p>Dependiendo la criticidad del incidente se presentan tiempos mas largos o cortos pero el promedio es de 1 hora</p>	<p>X</p>
<p>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: (El solicitante puede proporcionar más explicaciones a continuación) <i>With respect to access controls for each user's workstation, select the description which best reflects the Applicant's posture: (The Applicant can provide further explanation below)</i></p> <p>Ningún empleado está en el grupo de administradores ni tiene acceso de administrador local a sus estaciones de trabajo. <i>No employees are in the Administrators' group or have local admin access to their workstations.</i></p> <p>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 excepciones se documentan. <i>Applicant's policy is that employees by default are not in the Administrators' group and do not have local admin access; all exceptions to the policy are documented.</i></p> <p>Algunos de los empleados del Solicitante están en el grupo de administradores o son administradores locales.!! <i>Some of Applicant's employees are in the Administrators' group or are local admins.</i></p> <p>No sabe / <i>Do not know.</i></p> <p>Comentarios adicionales sobre los controles de acceso para estaciones de trabajo: / <i>Additional commentary on access controls for workstations:</i></p> <p>Solo personal autorizado y de tecnología cuenta con accesos adicionales de administrador, los cuales son autorizados por el area de riesgos acorde a su funcion.</p>	<p>X</p>
<p>11 Con respecto a la protección de credenciales privilegiadas, seleccione todas las que correspondan con la postura del Solicitante:!! <i>With respect to protecting privileged credentials, select all that apply with respect to the Applicant's posture:</i></p> <p>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.). <i>System administrators at the Applicant have a unique, privileged credential for administrative tasks (separate from their user credentials for everyday access, email, etc.).</i></p> <p>Las cuentas con privilegios (incluidos los administradores de dominio) requieren autenticación multifactor. <i>Privileged accounts (including Domain Administrators) require multifactor authentication.</i></p> <p>Las cuentas privilegiadas se guardan en un lugar seguro con contraseña que requieren que el usuario "revise" la credencial (que luego se rota). <i>Privileged accounts are kept in a password safe that require the user to "check out" the credential (which is rotated afterwards).</i></p> <p>Hay un registro de todo el uso de la cuenta con privilegios durante al menos los últimos treinta días.!! <i>There is a log of all privileged account use for at least the last thirty days. !!</i></p> <p>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). <i>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/ Domain Controllers).</i></p> <p>Ninguna de las anteriores / <i>None of the above.</i></p> <p>Comentarios adicionales sobre la protección de credenciales con privilegios: / <i>Additional commentary on protecting privileged credentials:</i></p> <p>Se tiene implementado el servicio de PAM para el manejo de estas cuentas privilegiadas</p>	<p>X</p> <p>X</p>
<p>12 Indique el uso de Microsoft Active Directory por parte del solicitante (en todos los dominios o "forests"): <i>Indicate the Applicant's use of Microsoft Active Directory (across all domains/forests):</i></p> <p>El Solicitante no utiliza Microsoft Active Directory (indicar a la derecha) <i>Applicant does not use Microsoft Active Directory (indicate to the right)</i></p> <p>Número de cuentas de usuario en el grupo Administradores de dominio (incluya cuentas de servicio, si las hay, en este total):!! <i>Number of user accounts in the Domain Administrators group (include service accounts - if any - in this total):!!</i></p> <p>Número de cuentas de servicio en el grupo Administradores de dominio: ("cuenta de servicio" significa una cuenta de usuario creada específicamente para que una aplicación o servicio interactúe con otros equipos unidos a un dominio): <i>Number of service accounts in the Domain Administrators group: ("service account" means a user account created specifically for an application or service to interact with other domain-joined computers):</i></p> <p>Comentario adicional sobre el número de administradores de dominio: / <i>Additional commentary on the number of Domain Administrators:</i></p> <p>Se tienen cuentas privilegiadas con servicios específicos y todas se encuentran documentadas</p>	<p>11</p> <p>7</p>
<p>13 ¿Cuántos usuarios tienen cuentas privilegiadas persistentes para endpoints (servidores y estaciones de trabajo)? (Para los propósitos de esta pregunta, "cuentas privilegiadas" significa derechos para configurar, administrar y brindar soporte a estos endpoints; no se deben incluir los usuarios que deben "verificar" las credenciales. El Solicitante puede proporcionar una explicación más detallada a continuación) <i>How many users have persistent privileged accounts for endpoints (servers and workstations)? (For the purposes of this question, "privileged accounts" means entitlements to configure, manage and otherwise support these endpoints; users who must "check out" credentials should not be included. The Applicant can provide further explanation below)</i></p> <p>Introduzca un número entero: / <i>Please enter an integer:</i></p> <p>Comentario adicional sobre el número de cuentas con privilegios: / <i>Additional commentary on the number of privileged accounts:!!</i></p> <p>Los usuarios Privilegiados con permisos específicos son cuentas administradas por el area de mesa de servicio, impresión y personal nivel 2 y 3</p>	<p>26</p>
<p>14 Con respecto a la seguridad de los sistemas externos, seleccione todo lo que corresponda a la postura del Solicitante: <i>With respect to the security of externally facing systems, select all that apply to the Applicant's posture:</i></p> <p>El Solicitante realiza una prueba de penetración al menos una vez al año para evaluar la seguridad de sus sistemas externos <i>Applicant conducts a penetration test at least annually to assess the security of its externally facing systems.</i></p> <p>El Solicitante tiene un firewall de aplicaciones web ("Web Application Firewall" - WAF) frente a todas las aplicaciones externas y está en modo de bloqueo. <i>Applicant has a Web Application Firewall (WAF) in front of all externally facing applications, and it is in blocking mode.</i></p> <p>El Solicitante utiliza un servicio externo para monitorear su superficie de ataque (sistemas externos/orientados a Internet). <i>Applicant uses an external service to monitor its attack surface (external/Internet facing systems).</i></p> <p>Ninguna de las anteriores / <i>None of the above.</i></p>	<p>X</p> <p>X</p> <p>X</p>
<p>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)? <i>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)?</i></p> <p>No hay ninguna directiva definida para cuando se deben implementar revisiones. / <i>There is no defined policy for when patches must be deployed.</i></p> <p>Dentro de 24 horas. / <i>Within 24 hours.</i></p> <p>24-72 horas/hours 3-7 días/days > 7 días/days</p> <p>Comentario adicional sobre los tiempos de destino para la aplicación de parches: / <i>Additional commentary on target times for patching:</i></p>	<p>X</p>
<p>16 ¿Cuál es el % de cumplimiento de los propios estándares del Solicitante al año para la implementación de parches críticos? (El solicitante puede proporcionar más explicaciones a continuación)!! <i>What is the Applicant's year to date compliance with its own standards for deploying critical patches? (The Applicant can provide further explanation below)</i></p> <p>Applicant does not track this metric/Do not know / <i>Applicant does not track this metric/Do not know</i></p> <p>>95% 90-95% 80-90% <80%</p> <p>Comentarios adicionales sobre el cumplimiento de los parches: / <i>Additional commentary on patching compliance:</i></p>	<p>X</p>
<p>17 Con respecto a las capacidades de supervisión de la red del Solicitante, seleccione todas las que correspondan:!! <i>With respect to the Applicant's network monitoring capabilities, select all that apply:</i></p> <p>El Solicitante utiliza una herramienta de monitoreo de eventos e información de seguridad (SIEM) para correlacionar la salida de múltiples herramientas de seguridad. <i>Applicant uses a security information and event monitoring (SIEM) tool to correlate the output of multiple security tools.</i></p> <p>El Solicitante monitorea el tráfico de la red en busca de transferencias de datos anómalas y potencialmente sospechosas. <i>Applicant monitors network traffic for anomalous and potentially suspicious data transfers.</i></p> <p>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). <i>Applicant monitors for performance and storage capacity issues (such as high memory or processor usage, or no free disk space).</i></p> <p>El Solicitante tiene herramientas para monitorear la pérdida de datos (DLP) y están en modo de bloqueo.!! <i>Applicant has tools to monitor for data loss (DLP) and they are in blocking mode.</i></p>	<p>X</p> <p>X</p> <p>X</p>

