CyberEdge® Supplemental Questionnaire - Ransomware

Este cuestionario complementario es aplicable a la cobertura CyberEdge®. Como se usa en este documento, "**Solicitante**" incluye a la **Compañía** que solicita la cobertura CyberEdge® y sus subsidiarias.

Note: 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 especificarán "seleccione todo lo que corresponda".

Nombre Completo del Solicitante	Fogacoop

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.	X
	El Solicitante utiliza ataques de phishing simulados para probar la conciencia de seguridad cibernética de los empleados al menos una vez al año.	X
	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).	X
	El Solicitante "etiqueta" o marca los correos electrónicos de fuera de la organización.	
	El Solicitante tiene un proceso para reportar correos electrónicos sospechosos a un equipo de seguridad interno para que los investigue.	X
	Ninguna de las anteriores	
	Comentarios adicionales sobre los esfuerzos de la compañía para mitigar el phishing	
	Se comparten correos de alertas que se reciben de la SFC, CSIRT y otras fuentes	
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	X
	No	
	Si la respuesta es "Sí", describa los pasos principales para responder:	
	No es precisamente unproceidmiento, pero si una oboigación de los funcionarios reportar los incidentes y eventos. Esta documentado como responsabilidad dentro del manual de funciones de cada cargo	
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.	X
	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.	X
	El **Solicitante** utiliza una solución de filtrado web que evita que los empleados visiten páginas web sospechosas o maliciosas.	X
	El **Solicitante** bloquea dominios no categorizados y recién registrados mediante servidores proxy web o filtros DNS.	X
	El **Solicitante** utiliza una solución de filtrado web que bloquea las descargas sospechosas o maliciosas conocidas, incluidos los ejecutables.	X
	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	
	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).	X
	Ninguna de las anteriores	
	Comentarios adicionales sobre los esfuerzos para bloquear sitios web y/o correo electrónico maliciosos:	
	Sensibilización y concienciación a usuarios, SOPHOS Endpoint Protection (antivirus, antimalware, Randsomware, Exploit, Virus)	
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)	
	El acceso remoto a los recursos corporativos requiere un nombre de usuario y una contraseña válidas (autenticación de factor único).	X
	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.	
	El **Solicitante** no proporciona acceso remoto a los empleados.	

	Comentarios adicional sobre autenticación para empleados:	
	El acceso remoto a las aplicaciones se realiza mediante diferentes capas de seguridad mediante VPN con control de usuairo y contraseña, seguido de acceso a escritorio remoto igualmente con usario y contraseña. Estando en el ambiente, las aplicaciones requieren adicionalmente usuario y contraseña. Cada usuario tiene acceso limitado da los activos de informción teniendo en cuenta su perfilamiento	
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).	X
	La autenticación multifactor está implementada para algunos tipos de acceso remoto a los recursos corporativos, pero no para todos.	X
	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	
	Comentarios adicional sobre autenticación para contratistas y proveedores independientes:	
	Fogacoop no tiene contratado terceros para que ejecuten y administren sus procesos. No tiene tercerización de procesos. Se provee acceso remoto y bajo control de usuarios, cotraseñas y delimitación a los activos a proveedores de soporte, bajo el control y seguimiento de un supervisor del área de TI.	
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)	
	No aplicable (el **Solicitante** no utiliza la autenticación multifactor)	X
	No; La implementación multifactor del **Solicitante** no cumple los criterios anteriores.	
	Sí; la implementación multifactor del solicitante cumple con los criterios anteriores.	
	Comentarios adicionales sobre la implementación de la autenticación multifactor:	
	N.A. no se administran diferentes dispositivos para dar acceso segregado a diferentes activos de información. La entidad hace uso de servicios que prestan terceros a traves de sus redes (portales bancarios, firmas digitales) que hace uso de doble factor de autenticación (contraseña, usuario y token). no obstante la sgeuridad de estos accesos la proporciona los mismos proveedores.	
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.	X
	El **Solicitante** utiliza herramientas de seguridad de endpoints con capacidades de detección del comportamiento y mitigación de vulnerabilidades.	X
	El **Solicitante** tiene un grupo interno que supervisa la salida de las herramientas de seguridad en los endpoints e investiga cualquier anomalía.	X
	Ninguna de las anteriores	
	Comentario adicional sobre las capacidades de seguridad de los endpoints:	
	La solución de Enpoint Protection, se adminsitra de manera centralizada por parte del administrador de seguridad de la red contratado. Este proveedor realiza seguimiento y analisis de amenzas y eventos y reporta a Fogacoop,	
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** 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:	
	Se cuenta con un Servicio de DATACENTER que incluye Seguridad Gestionada mediante un SOC	
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)	
	El **Solicitante** no rastrea esta métrica/No sabe	
	<30 minutos	
	30 minutos-2 hooras	X
	2-8 horas	
	>8 horas	
	Comentario adicional sobre el tiempo promedio para corregir:	

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)	
	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 excepciones se documentan.	
	Algunos de los empleados del **Solicitante** están en el grupo de administradores o son administradores locales.	x
	No sabe	
	Comentarios adicionales sobre los controles de acceso para estaciones de trabajo:	
	En las estaciones de trabajo cada funcionario tiene asignado un usuario mediante un Directorio Activo quien es quien controla el acceso y políticas. Solamente el responsable de Seguridad Informática de TI es quien gestiona el acceso administrador tanto de red como local de los equipos de computo,	
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.).	X
	Las cuentas con privilegios (incluidos los administradores de dominio) requieren autenticación multifactor.	
	Las cuentas privilegiadas se guardan en un lugar seguro con contraseña que requieren que el usuario "revise" la credencial (que luego se rota).	X
	Hay un registro de todo el uso de la cuenta con privilegios durante al menos los últimos treinta días.	X
	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).	X
	Ninguna de las anteriores	
	Comentarios adicionales sobre la protección de credenciales con privilegios:	
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)	
	Número de cuentas de usuario en el grupo Administradores de dominio (incluya cuentas de servicio , si las hay, en este total):	2
	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):	
	Comentario adicional sobre el número de administradores de dominio:	
	Las cuentas de servicio no hacen parte del grupo administrador	
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)	
	Introduzca un número entero:	1
	Comentario adicional sobre el número de cuentas con privilegios:	
	El servicio de Endpoint es tercerizado	
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	
	El **Solicitante** tiene un firewall de aplicaciones web ("Web Application Firewall" - WAF) frente a todas las aplicaciones externas y está en modo de bloqueo.	X
	El **Solicitante** utiliza un servicio externo para monitorear su superficie de ataque (sistemas externos/orientados a Internet).	X
	Ninguna de las anteriores	
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)?	
	No hay ninguna directiva definida para cuando se deben implementar revisiones.	
	Dentro de 24 horas.	
	24-72 horas.	X
	3-7 días.	

	> 7 días.	
	Comentario adicional sobre los tiempos de destino para la aplicación de parches:	
	Hace parte de los ANS que se tienen establecidos con el proveedor del Datacenter	
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	X
	>95%	
	90-95%	
	80-90%	
	<80%	
	Comentarios adicionales sobre el cumplimiento de los parches:	
	Los parches son aplicados en la medida de su publicación y esto se realiza de manera automática en las estaciones de trabajo.	
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.	X
	El **Solicitante** monitorea el tráfico de la red en busca de transferencias de datos anómalas y potencialmente sospechosas.	X
	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).	X
	El **Solicitante** tiene herramientas para monitorear la pérdida de datos (DLP) y están en modo de bloqueo.	
	Ninguna de las anteriores	
	Comentarios adicionales sobre la supervisión de la red:	
18	Con respecto a limitar el movimiento lateral, seleccione todo lo que se aplique a la postura del **Solicitante**: (El solicitante puede proporcionar más explicaciones a continuación)	
	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).	X
	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).	
	El **Solicitante** ha implementado reglas de firewall de host que impiden el uso de RDP para iniciar sesión en estaciones de trabajo.	X
	El **Solicitante** ha configurado todas las cuentas de servicio para denegar los inicios de sesión interactivos.	X
	Ninguna de las anteriores	
	Comentario adicional sobre la segmentación:	
19	Introduzca la fecha del último ejercicio ransomware del **Solicitante**; marque la casilla si no se ha llevado a cabo ninguno.	
	Fecha: 25-09-2022 (PHISHING)	X
	No se ha realizado ningún ejercicio ransomware. (Se ha realizado ejercicios de Phishing)	X
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.	
	No	
	Sí	x
	Principales pasos realizado por el tercero:	
	El plan de respuesta corresponde al previsto en el tratamiento de incidentes. Detectar, reportar, contener, tranferir caso a Datacenter para solución, contactar autoridades en casos críticos	
21	Con respecto a la verificación de la eficacia de los controles de seguridad, seleccione todo lo que se aplica al **Solicitante**: (El solicitante puede proporcionar más explicaciones a continuación)	
	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.	
	El **Solicitante** ha contratado a una parte externa para simular actores de amenazas y probar controles de seguridad en el último año. (Ver observación- Para implementar en 2023)	X
	Ninguna de las anteriores	

	Comentario adicional sobre la verificación de los controles:	
	Se tiene definido un plan de pruebas de efectividad de contorles a ejecutar durante el año 2023	
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	
	El **Solicitante** tiene una política de recuperación ante desastres documentada, que incluye estándares para copias de seguridad basadas en la criticidad de la información.	x
	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.	
	Ninguna de las anteriores	
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.	
	4-24 horas.	
	1 to 2 días.	x
	2-7 días.	
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)	
	La estrategia de copia de seguridad del **solicitante** incluye copias de seguridad sin conexión almacenadas fuera del sitio	X
	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:	
	La copias de seguridad locales son resguardas en cintas en sitio externo y con DATA CENTER se tiene el servicio de Backup, siente este un DATACENTER TIER III	
25	¿El **Solicitante cuenta con** alguna política que todos los dispositivos portátiles utilizan cifrado de disco completo?	
	Sí	x
	No	
	Comentarios Adicionales:	
	En proceso de implementación	

ESTE CUESTIONARIO COMPLEMENTARIO SE INCORPORA Y FORMA PARTE DE CUALQUIER SOLICITUD DE COBERTURA DE RIESGOS CIBERNÉTICOS POR PARTE DEL SOLICITANTE. TODAS LAS DECLARACIONES Y GARANTIAS REALIZADAS POR EL SOLICITANTE EN RELACIÓN CON DICHA SOLICITUD SE APLICAN TAMBIEN A LA INFORMACION PROPORCIONADA EN ESTE CUESTIONARIO ADICIONAL.

EN CASO DE QUE EL ASEGURADO EMITA UNA POLÍLZA, EL SOLICITANTE ACEPTA QUE DICHA POLÍZA SE EMITE EN FUNCIÓN DE LA VERDAD DE LAS DECLARACIONES Y REPRESENTACIONES EN ESTE CUESTIONARIO COMPLEMENTARIO O INCORPORADO POR REFERENCIA EN EL PRESENTE DOCUMENTO. CUALQUIER DECLARACIÓN FALSA, OMISIÓN, OCULTACIÓN O DECLARACIÓN INCORRECTA DE UN HECHO MATERIAL, EN ESTE CUESTIONARIO COMPLEMENTARIO, INCORPORADO POR REFERENCIA O DE OTRO MODO, SERÁ MOTIVO DE LA RESCISIÓN DE CUALQUIER POLÍZA EMITIDA.

EL ABAJO FIRMANTE ACEPTA, GARANTIZA Y REPRESENTA QUE ES UN REPRESENTANTE DEBIDAMENTE AUTORIZADO DEL SOLICITANTE, Y ESTÁ TOTALMENTE AUTORIZADO PARA RESPONDER Y HACER DECLARACIONES Y REPRESENTACIONES POR Y EN NOMBRE DEL SOLICITANTE.

Firma: MARIA ELENA GRUESO RODRIGUEZ — Firmado digitalmente por MARIA ELENA GRUESO RODRIGUEZ Fecha: 2022.10.11 16:09:56 -05'00'

MARÍA ELENA GRUESO RODRÍGUEZ

Fecha: OCTUBRE 11 DE 2022

Título: DIRECTORA - REPRESENTANTE LEGAL

Organización: FONDO DE GARANTÍAS DE ENTIDADES COOPERATIVAS - FOGACOOP