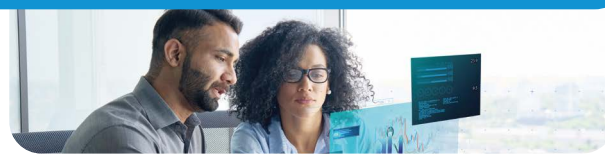
seguros mundial®

PRODUCTO CYBER EMPRESARIAL
FORMULARIO DE RANSOMWARE

NIT 860.037.013-6
Calle 33 # 6B - 24, pisos 1, 2 y 3
Tel: (601) 327 4712 / 13
Bogotá D.C. - Colombia
Somos Grandes Contribuyentes
IVA Régimen Común - Autorretenedores

Fecha
D M A
Ciudad



Este documento permite a Seguros Mundial S.A. reunir la información necesaria para evaluar los riesgos relacionados con los sistemas de información del posible asegurado. Tenga en cuenta que la realización de este breve formulario de solicitud no compromete a Seguros Mundial S.A., ni al posible asegurado, a suscribir una póliza de seguro. Si la política de seguridad de los sistemas de información de las empresas/filiales de los posibles asegurados varía, diligencie el formulario de solicitud para cada posible asegurado. Tenga en cuenta también que puede llegar a ser necesaria más información, incluyendo un formulario de solicitud adicional.

Este documento constituye una solicitud de seguro y, por lo tanto, puede o no ser aceptada por la aseguradora. Una vez analizados los antecedentes proporcionados por el representante del asegurado. La aseguradora se reserva el derecho de proponer alternativas de cobertura. Por lo tanto, es posible que la aceptación difiera parcialmente con los términos de la solicitud. Celebrado el contrato de seguro, esta propuesta se convertirá en parte integral de la póliza. La veracidad en las declaraciones del representante del asegurado se considerará elemento esencial de la propuesta, en consecuencia, es fundamental que todas las preguntas sean contestadas correcta y completamente.

Por favor diligencie todas y cada una de las siguientes preguntas que se hacen.

Información de la compañía

Nombre de la compañía
Página web
Sede de la empresa (dirección, ciudad, país, código postal)
Año de fundación **Número de empleados**

Indique los datos de contacto del CISO del cliente o de otro miembro del personal responsable de la seguridad de los datos y la red

Nombre (nombre y apellido) **Rol**
Email **Teléfono**

Tenga en cuenta que Seguros Mundial S.A. puede utilizar estos datos de contacto para apoyar a nuestros asegurados con información sobre servicios adicionales de seguridad cibernética, alertas de vulnerabilidad y otra información cibernéticos útiles.

Perfil de la compañía

1. Ingresos – Por favor, describa el volumen de ingresos que genera anualmente

Ingresos	Estimado año actual	Proyectado para el año siguiente
Ingresos globales/Ingresos brutos		
Porcentaje de ingresos globales generados actualmente en EE.UU. y Canadá	%	
Porcentaje de ingresos globales generados actualmente por las ventas en línea	%	

2. Actividades de negocio - Describa a qué se dedica su empresa para generar el volumen de negocio indicado anteriormente, incluidas las actividades de las subsidiarias

3. ¿Su empresa es una filial, una franquicia o una entidad menor de una organización mayor? **Sí** **No**

En caso afirmativo, indique los detalles

4. ¿Proporciona usted algún servicio a, o comercia con, personas u organizaciones de territorios sancionados, incluyendo entre otros, ¿Irán, Siria, Sudán del Norte, la región de Crimea y Cuba, o cualquier territorio que está sujeto a ciertas restricciones de sanciones de EE.UU., la UE, las Naciones Unidas u otros países? **Sí** **No**

5. Alcance de las actividades - Tiene alguna empresa o filial domiciliada fuera del país de sede principal, para la que se requiera cobertura? **Sí** **No**

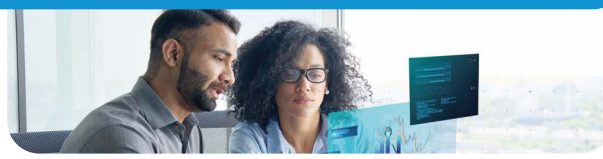
a. En caso afirmativo, proporcione información adicional sobre la ubicación de estas entidades y el porcentaje de ingresos que genera cada una de ellas. Si necesita más espacio, inclúyalo como anexo a esta propuesta.

Nota: Esta información es importante para asegurar que cada una de sus entidades es elegible para la cobertura en los países en los que opera

Comentarios adicionales sobre las operaciones de negocio

seguros mundial®

PRODUCTO CYBER EMPRESARIAL
FORMULARIO DE RANSOMWARE



NIT 860.037.013-6
Calle 33 # 6B - 24, pisos 1, 2 y 3
Tel: (601) 327 4712 / 13
Bogotá D.C. - Colombia
Somos Grandes Contribuyentes
IVA Régimen Común - Autorretenedores

Privacidad de los datos

1. **¿Aproximadamente a cuántas personas y organizaciones únicas tendría que notificar en caso de una violación de Información de Identificación Personal (IIP)?**

2. **Aproximadamente, ¿de cuántas personas y organizaciones únicas tiene usted:**
   a. Información de la tarjeta de pago o de la cuenta bancaria
   b. Registros de información clínica
3. **¿Se procesa información de tarjetas de pago (PCI) en el transcurso de su negocio?** **Sí** **No**
   a. En caso afirmativo, ¿cuál es el número estimado de transacciones PCI que procesa anualmente?
   b. Por favor, describa su nivel de cumplimiento de PCI DSS (o el de su subcontratista)
   Nivel 1 Nivel 2 Nivel 3 Nivel 4 No cumple (describa)

Seguridad de los datos y de la información

1. **Por favor, indique si cuenta con las siguientes prácticas de planificación, recursos y gobernanza de datos y riesgos cibernéticos:**
   a. Política formal de privacidad aprobada por el departamento legal y la gerencia **Sí** **No**
   b. Política formal de seguridad de la información aprobada por legal y la gerencia **Sí** **No**
   c. Política formal de clasificación de datos **Sí** **No**
   d. Personal dedicado al gobierno de la seguridad de los datos y del sistema **Sí** **No**
   e. Un plan formal de respuesta a incidentes cibernéticos específicos probado al menos una vez al año **Sí** **No**
   f. Monitoreo formal del cumplimiento de las leyes y normas de privacidad **Sí** **No**
   g. Las políticas de seguridad cibernética se gestionan a nivel central/superior para todas las subsidiarias, quienes deben cumplir con las mismas **Sí** **No**

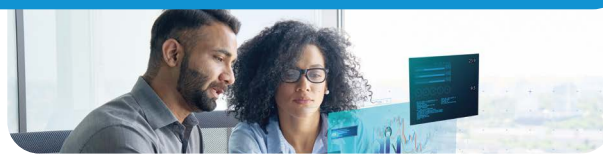
   Comentario adicional

2. **¿Ha identificado todas las normas de privacidad y seguridad de la red y los estándares de cumplimiento aplicables a las regiones en las que opera?**
   Sí **No** **Parcialmente**
3. **¿Ha evaluado el cumplimiento de estos requisitos en los últimos 12 meses?** **Sí** **No** **Parcialmente**
4. **Proporcione comentarios adicionales sobre cualquier incumplimiento de las Leyes y Normas de Privacidad pertinentes en las jurisdicciones aplicables, junto con los planes establecidos para remediarlo:**
5. **¿Usted y otros en su nombre o bajo su dirección recolectan, almacenan o transmiten información biométrica, incluyendo, pero no limitándose a las huellas dactilares, escáneres de retina o relojes de tiempo que se basan en identificadores individuales?** **Sí** **No**
   En caso afirmativo, por favor, complete las preguntas complementarias de "Información biométrica" al final de este documento.
6. **Por favor, complete las siguientes preguntas en relación con el almacenamiento, la protección o la minimización de la Información de Identificación Personal (IIP):**
   a. Si la IIP está segmentada, indique el número total de individuos únicos que existirían en una sola base de datos o repositorio
   b. ¿Se limita el acceso a las bases de datos con IIP a la condición de que sea necesario conocerlas? **Sí** **No**
   c. Indique qué otros controles protegen o minimizan su IIP:
   Microsegmentación Anonimización de datos Seudonimización de datos Tokenización de datos
   Cifrado a nivel de base de datos Cifrado en tránsito Soluciones Empresariales o Integradas de Prevención de Pérdida de Datos (DLP)
   Otro
7. **¿Subcontrata el tratamiento/procesamiento de la IIP a uno o varios procesadores de datos?** **Sí** **No** **Parcialmente**
   a. ¿Mantiene contratos por escrito con dichos proveedores en todo momento? **Sí** **No** **Parcialmente**
   b. ¿Estos contratos establecen qué parte es responsable de responder a una violación de datos? **Sí** **No** **Parcialmente**
   c. ¿Renuncia a los derechos de indemnización contra los procesadores de datos en caso de violación de datos? **Sí** **No** **Parcialmente**

   Comentario adicional sobre el almacenamiento y la recolección de IIP:

seguros mundial®

PRODUCTO CYBER EMPRESARIAL
FORMULARIO DE RANSOMWARE



NIT 860.037.013-6
Calle 33 # 6B - 24, pisos 1, 2 y 3
Tel: (601) 327 4712 / 13
Bogotá D.C. - Colombia
Somos Grandes Contribuyentes
IVA Régimen Común - Autorretenedores

Controles técnicos y procesos

Estructura de la red y Controles de Acceso

1. **¿Los sistemas y aplicaciones críticas están alojados de forma centralizada?** Sí ○ No ○ Parcialmente ○
2. **Detalle cómo se ha estructurado o segmentado su red para minimizar el movimiento lateral de malware o de usuarios dentro de su organización, o minimizar la posibilidad de que múltiples servicios sean impactados por la misma situación o por la misma vulnerabilidad:**

   Utiliza:

   ○ VLAN ○ Air-gap ○ Firewalls basados en el host ○ Configuración del firewall (lista de control de acceso) ○ Redes definidas por software (SDN)
   ○ Controles de acceso de mínimo privilegio ○ Otro
3. **Por favor, indique si usted tiene implementada cualquiera de los siguientes:**
   - ○ Pruebas de penetración externas realizadas al menos anualmente
   - ○ Pruebas de penetración internas del sistema realizadas al menos una vez al año
   - ○ Los Firewalls de Aplicaciones Web (WAF) se aplican a la mayoría de las aplicaciones críticas expuestas al exterior
4. **¿Permite que los dispositivos móviles (incluidos computadores portátiles, tabletas y teléfonos inteligentes) accedan a las aplicaciones y recursos de la empresa o de la red?**

   Sí ○ **No** ○

   a. ¿Qué porcentaje de dispositivos móviles son Dispositivos Gestionados, o ha habilitado y aplicado un producto de Gestión de Dispositivos Móviles?

   1. Computadores portátiles, tablets y smarphones de la empresa % ○ N/A
   2. Traiga su propio dispositivo (BYOD) (incluidos computadores portátiles, tabletas y teléfonos inteligentes) % ○ N/A
5. **¿Tiene alguna parte de su red corporativa capacidades para el acceso remoto?** **Sí** ○ **No** ○

   En caso afirmativo, por favor, complete lo siguiente:

   a. ¿Cómo gestiona el acceso remoto seguro a su red corporativa? (seleccione todos los que correspondan)

   ○ VPN (Red Privada Virtual) ○ Autenticación de Múltiples Factores
   ○ SSO (Single Sign-on) vía MFA ○ ZTNA (Acceso de Confianza Cero a la Red)
   ○ Cifrado de tráfico ○ Otro

   b. ¿Lo anterior se aplica a los empleados estándar, a los contratistas, a los vendedores, a los proveedores y a los usuarios privilegiados que tienen acceso remoto a su red corporativa?

   Sí ○ **No** ○ **Parcialmente** ○

   Por favor, detalle cualquier excepción a lo anterior, o proporcione comentarios adicionales:
6. **Por favor, detalle su uso del Protocolo de Escritorio Remoto (RDP):**

   ○ No se utiliza RDP en absoluto ○ Se utiliza RDP para el acceso remoto
   ○ Se limita el uso de RDP sólo para uso interno ○ El RDP se utiliza con otro fin:

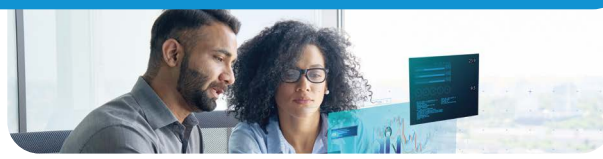
   a. Si se utiliza el RDP de alguna manera, ¿cuáles de los siguientes elementos se implementan? (seleccione todo lo que corresponda)

   ○ VPN (Red Privada Virtual) ○ Autenticación de Múltiples Factores ○ NLA (Autentificación a Nivel de Red)
   ○ Establecimiento de honeypots (señuelos) para RDP ○ Otro

Directorio, Dominios y Cuentas

7. **¿Dispone de un programa formal de Gestión de Identidades y Control de Acceso?** Sí ○ No ○
8. **Por favor, detalle le número de:**

   a. Cuentas de servicio
   b. Usuarios con acceso de administrador
   c. Usuarios que tienen acceso administrativo persistente a estaciones de trabajo y servidores distintos de los suyos
   d. Usuarios con privilegios que tienen acceso completo a su servicio de directorio, incluido el Dominio de Directorio Activo
9. **Por favor, detalle por qué es necesario este número de Cuentas Privilegiadas, y cualquier acción planeada para reducir este número:**



NIT 860.037.013-6
Calle 33 # 6B - 24, pisos 1, 2 y 3
Tel: (601) 327 4712 / 13
Bogotá D.C. - Colombia
Somos Grandes Contribuyentes
IVA Régimen Común - Autorretenedores

10. Por favor, indique otros controles establecidos para la gestión de las cuentas:

- Las cuentas locales y de dominio se auditan periódicamente para comprobar la creación no autorizada de nuevas cuentas
- Los registros de acceso se almacenan durante al menos 90 días
- Los administradores de red tienen cuentas "normales" y "privilegiadas" separadas con autenticación independiente
- Se utilizan Estaciones de Trabajo con Acceso Privilegiado
- Las Cuentas Privilegiadas y los servicios de directorio (incluido el Directorio Activo) se supervisan en busca de actividad inusual
- Se controla el uso de Cuentas Privilegiadas mediante una solución de Gestión de Accesos Privilegiados
- El acceso privilegiado requiere una Autenticación Multi-Factor separada para el acceso interno o en la red

Por favor, detalle cualquier excepción a lo anterior o proporcione comentarios adicionales relacionados con los controles de acceso, los servicios de directorio (incluyendo el Dominio de Directorio Activo) y las Cuentas Privilegiadas:

Autenticación

11. ¿En los casos en los que ha implementado la Autenticación de Factores Múltiples, se ha configurado esta solución de manera que la vulneración de un solo dispositivo sólo comprometa a un solo factor de autenticación? **Sí** **No** **N/A**

Comentario adicional:

Seguridad del correo electrónico

12. Por favor, detalle cómo gestiona la seguridad de la actividad de correo electrónico (seleccione todo lo que corresponda)):

- MFA es necesaria para el correo electrónico alojado en la nube o en la web
- Los correos electrónicos se etiquetan como "externos" o similar según aplique
- El Sender Policy Framework (SPF) está implementado/habilitado
- El Correo identificado con claves de dominio (DKIM) está implementado/habilitado
- Todo el correo electrónico entrante pasa por una puerta segura de correo electrónico
- Todo el correo electrónico entrante se escanea y se filtra en busca de malware
- Todos los correos electrónicos sospechosos se ponen automáticamente en cuarentena
- Se utiliza el Sandboxing para investigar los archivos adjuntos al correo electrónico
- Los correos electrónicos externos que se consideran sensibles se envían de forma segura
- Todos los empleados reciben formación sobre los riesgos del phishing y otras amenazas de ingeniería social
- Las macros de Microsoft Office están deshabilitadas por defecto
- Otro

Continuidad del Negocio y Recuperación de Desastres

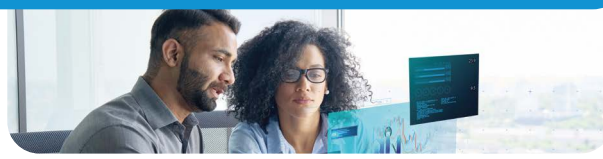
13. ¿Cuenta con un Plan de Continuidad de Negocio formal que aborde escenarios cibernéticos, probado anualmente? **Sí** **No**

14. ¿Cuenta con un Plan de Recuperación de Desastres formal que aborde escenarios cibernéticos, probado anualmente? **Sí** **No**

15. Por favor, suministrar detalles adicionales sobre estrategias para Ransomware en cuanto a protección de copias de seguridad para la recuperación de desastres:

- Tecnología de copia de seguridad inmutable o de Escritura Única y Lectura Múltiple (WORM)
- Copias de seguridad completamente Offline / Air-gapped (cinta / discos no montados-externos) desconectadas del resto de su red
- Acceso restringido a través de una Cuenta Privilegiada separada que no está conectada al Directorio Activo u otros dominios
- Acceso restringido a las copias de seguridad mediante MFA
- Cifrado de las copias de seguridad
- Copias de seguridad alojadas en la nube segmentadas de su red
- Otro

NIT 860.037.013-6
Calle 33 # 6B - 24, pisos 1, 2 y 3
Tel: (601) 327 4712 / 13
Bogotá D.C. - Colombia
Somos Grandes Contribuyentes
IVA Régimen Común - Autorretenedores



16. Por favor, indique si las siguientes prácticas de planificación y pruebas de copias de seguridad le son aplicables:

- Se realizan pruebas de restauración completa a partir de una copia de seguridad
- Se comprueba la recuperabilidad de los datos
- Se analiza la integridad de los datos durante las pruebas
- El plan de restauración incluye escenarios específicos de ransomware
- Se analizan los datos en busca de malware antes de realizar la copia de seguridad
- Existen procedimientos de copia de seguridad para los registros de correo electrónico.

17. Describa los sistemas de información, aplicaciones o servicios (tanto internos como externos) de los que más depende para el funcionamiento de su empresa:

En cuanto a los servicios subcontratados, estos pueden incluir servicios en la nube, alojamiento de datos, servicios de aplicaciones empresariales, co-ubicación, copia de seguridad de datos, almacenamiento de datos, procesamiento de datos o cualquier tipo similar de subcontratación en materia de informática o sistemas

Nombre del Sistema, aplicación o servicio	Nombre del proveedor (si es subcontratado) Si es interno, ponga "N/A"	¿Se ha realizado un análisis de impacto empresarial (BIA)?

18. ¿Mantiene sistemas alternativos para las aplicaciones críticas? **Sí** **No** **Parcialmente**

19. ¿Dispone de energía alternativa para los equipos de misión crítica o que generan ingresos? **Sí** **No**

20. ¿Tiene la posibilidad de adquirir ancho de banda adicional de proveedores alternativos? **Sí** **No**

21. ¿Utilizan y prueban generadores de energía de reserva, unidades de suministro doble u otros equipos para compensar los cortes o fallos de energía como parte de los planes de continuidad de la actividad o de recuperación de desastres?

22. ¿Sus desarrolladores de software reciben formación sobre los principios del desarrollo seguro de aplicaciones? **Sí** **No** **N/A**

23. Describa los procedimientos de control de calidad y de prueba que se aplican a cualquier programa informático nuevo (incluidas las actualizaciones y las nuevas versiones de los programas existentes) en su red (incluido el plazo mínimo para que un sistema nuevo o actualizado supere las pruebas de garantía de calidad antes de que entre en operación en su entorno de red de producción, al igual que procedimientos en entornos separados de desarrollo, prueba y aceptación)

Prevención, monitoreo y respuesta a incidentes

24. ¿Tiene implementados planes y protecciones para los ataques de denegación de servicio distribuidos (DDoS)? **Sí** **No**

25. ¿Cómo previenen, controlan y responden a los incidentes y alertas cibernéticas? (seleccione todo lo que corresponda)

- Sistema de Detección de Intrusos
- Sistema de Prevención de Intrusiones
- Filtrado de URL o Filtrado Web
- Aislamiento y Contención de Aplicaciones
- Solución de Orquestación, Automatización y Respuesta de Seguridad (SOAR)
- Servicio de Protección del Sistema de Nombres de Dominio (DNS)
- Utilización de fuentes o servicios de Inteligencia de Amenazas
- Antimalware y antivirus avanzados o de nueva generación con Análisis Heurístico
- Revisiones manuales del registros (log)
- Centro de Operaciones de Seguridad (SOC) en funcionamiento
- Servicio de firewall gestionado
- Herramienta de Gestión de Eventos e Información de Seguridad (SIEM)

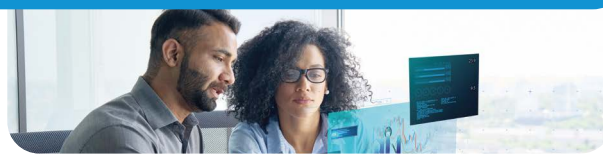
- Protección Avanzada de Endpoints
  - Endpoint Detection and Response (EDR)
  - Managed Detection and Response (MDR)
  - Extended Detection and Response (XDR)

  Proveedor(es)

Porcentaje de puntos finales cubiertos por EDR, MDR, or XDR %

¿Está configurada esta herramienta para aislar o bloquear automáticamente la actividad?
Sí **No** **Parcialmente**

Otras herramientas o servicios de monitoreo (por favor detallar)



NIT 860.037.013-6
Calle 33 # 6B - 24, pisos 1, 2 y 3
Tel: (601) 327 4712 / 13
Bogotá D.C. - Colombia
Somos Grandes Contribuyentes
IVA Régimen Común - Autorretenedores

26. ¿Las alertas de las herramientas EDR, MDR o XDR se introducen en un Sistema de Gestión de Eventos e Información de Seguridad (SIEM), en una plataforma de Orquestación, Automatización y Respuesta de Seguridad (SOAR) o en un sistema de Protección Centralizada de Endpoints (o similar)? % N/A

Gestión de activos y configuraciones

27. ¿Mantiene un inventario de los activos de hardware y software? Sí No

a. ¿Qué porcentaje de sus activos está incluido en este inventario? %

b. ¿Qué porcentaje de sus activos están dentro del alcance de las actividades de escaneo de vulnerabilidades? %

28. ¿Con qué frecuencia realiza escaneos de vulnerabilidad? **Internos** **Externos**

29. ¿Asigna niveles de riesgo a cada activo de su inventario para priorizar las acciones de parcheo y acciones de gestión de vulnerabilidades? Sí No

30.

En caso afirmativo, describa el uso que hace de hardware, software o sistemas que han llegado al final de su vida útil o que no cuentan con soporte técnico:

a. ¿Algunos de estos procesos, sistemas o aplicaciones son críticos para el negocio? **Sí** **No**

b. ¿Almacenan o procesan información confidencial personal o corporativa en estos sistemas? **Sí** **No**

c. ¿Estos sistemas tienen restringido el acceso a Internet? **Sí** **No** **Parcialmente**

d. ¿Están estos sistemas segregados y aislados de otras partes de su red? **Sí** **No** **Parcialmente**

e. Por favor, indique qué sistemas al final de su vida útil o sin soporte técnico utiliza, para qué se usan y cuántos se usan en su empresa:

f. Por favor, describa para estos sistemas sus planes de retirada o actualización y plazos:

g. Por favor, describa otros controles de mitigación establecidos para minimizar el movimiento lateral partiendo de los sistemas no soportados a otros entornos dentro de su red:

31. ¿Escanea regularmente y desactiva los puertos y protocolos abiertos innecesarios? Sí No

32. ¿Dispone de un proceso formal de gestión de parches? Sí No

33. Plazos objetivo en función de la criticidad de la vulnerabilidad (Common Vulnerability Scoring System – CVSS)

Bajo días Medio días Alto días Crítico días

34. Por favor, detalle su nivel de cumplimiento de estos objetivos en los últimos 12 meses:

35. ¿Si no se puede aplicar un parche a tiempo, qué medidas toma para mitigar el riesgo de vulnerabilidad?

Comentarios adicionales sobre la gestión de activos y parches:

Gestión de riesgos de terceros

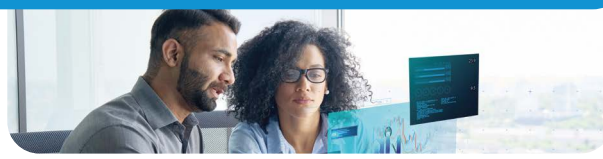
Para esta sección, los servicios de tecnología subcontratados, pueden incluir servicios en la nube, alojamiento de datos, servicios de aplicaciones empresariales, co-ubicación, copia de seguridad de datos, almacenamiento de datos, procesamiento de datos o cualquier tipo similar de subcontratación en materia de informática o sistemas

1. ¿Realiza evaluaciones basadas en el riesgo a aquellos proveedores de tecnología que son más críticos para su negocio? Sí No

2. Seleccione lo que se incluye en las evaluaciones de los proveedores, ya sea antes de la contratación o durante las auditorías:

- Revisión de la certificación de seguridad de la información
- Revisión de la certificación de resiliencia empresarial
- Pruebas de penetración
- Revisión de los procedimientos de copia de seguridad del proveedor
- Servicio de calificación de la seguridad cibernética
- Evaluación del acuerdo de nivel de servicio (SLA)
- Revisión de Autenticación Multi-Factor
- Se realiza una Evaluación de Impacto en la Protección de Datos
- Acuerdos de protección de datos incluidos en los contratos
- Otro

NIT 860.037.013-6
Calle 33 # 6B - 24, pisos 1, 2 y 3
Tel: (601) 327 4712 / 13
Bogotá D.C. - Colombia
Somos Grandes Contribuyentes
IVA Régimen Común - Autorretenedores



3. **¿Con qué frecuencia renuncia a su derecho de indemnización contra cualquier proveedor de tecnología de terceros en caso de interrupción del servicio?**
   - Nunca o con poca frecuencia
   - Algunas veces
   - Siempre o frecuentemente

   Otro comentario

Seguridad en la nube

4. **¿Utiliza aplicaciones, plataformas, infraestructuras u otros servicios en la nube?** **Sí** **No**
5. **¿Tiene una política formal de seguridad en la nube?** **Sí** **No** **N/A**
6. **Por favor, indique cuál de los siguientes elementos ha implementado para apoyar las iniciativas de seguridad en la nube:**
   - Agente de Seguridad de Acceso a la Nube (CASB)
   - Modelo de nube Perímetro de Servicio de Acceso Seguro (SASE) aplicado
   - Modelo de nube Acceso de Confianza Cero a la Red (ZTNA) aplicado
   - Single Sign On (SSO) utilizado para la autenticación en los servicios en la nube
   - Se requiere Autenticación Multi-Factor para acceder a las aplicaciones de nube críticas para el negocio
   - Se requiere Autenticación Multi-Factor para acceder a las aplicaciones en la nube que no son críticas para el negocio
   - Otro

Media

1. **¿El asesor jurídico ha examinado el uso de todas las marcas comerciales y de servicio incluido el uso de nombres de dominio y metaetiquetas, para asegurarse de que no infringen los derechos de propiedad intelectual de terceros?** **Sí** **No**
2. **¿Obtienen permisos o autorizaciones por escrito de terceros proveedores de contenido y colaboradores, incluidos los trabajadores autónomos, contratistas independientes y otros talentos?** **Sí** **No**
3. **¿Se cuenta con la participación de un asesor legal para revisar el contenido antes de su publicación o para evaluar si el contenido debe ser retirado tras una queja?** **Sí** **No**
4. **Contratan a proveedores externos, incluidas agencias de publicidad o de marketing, para crear o gestionar contenidos en su nombre?** **Sí** **No**

a. **En caso afirmativo, ¿exige acuerdos de indemnización o exención de responsabilidad a su favor?** **Sí** **No**

5. **¿Su política de privacidad, condiciones de uso, condiciones de servicio y otras política de los clientes han sido revisadas por un abogado?** **Sí** **No**

Historial de pérdidas

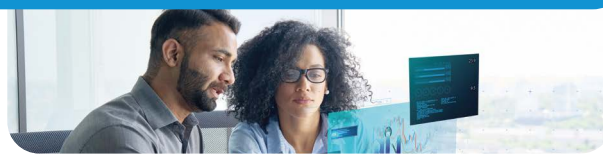
1. **Indique cuáles de los siguientes eventos ha experimentado en los últimos cinco años (no incluya los eventos que han sido mitigados por las medidas de seguridad existentes):**
   - Violación de datos
   - Incidente Cibernético malicioso en su contra
   - Evento de falla del sistema
   - Reclamación por Contenidos Electrónicos
   - Acciones regulatorias relacionadas con la seguridad de los datos o del sistema
   - Violación de datos a un proveedor externo que le presta servicios
   - Incidente Cibernético que afecte a un proveedor **externo**

a. En caso de respuesta afirmativa a alguna de las preguntas anteriores, por favor, indique:

Descripción de los siniestros/incidentes y fecha de ocurrencia:

Descripción del impacto financiero para su compañía:

Medidas de mitigación que ha tomado para evitar sucesos similares en el futuro:



NIT 860.037.013-6
Calle 33 # 6B - 24, pisos 1, 2 y 3
Tel: (601) 327 4712 / 13
Bogotá D.C. - Colombia
Somos Grandes Contribuyentes
IVA Régimen Común - Autorretenedores

2. **¿Tiene conocimiento de algún aviso, hecho, circunstancia o situación que pudiera calificarse como Violación de Datos, Incidente Cibernético, Evento de Falla del Sistema o que razonablemente pudiera dar lugar a cualquier Reclamación por Contenidos Electrónicos o acciones regulatorias relacionadas con la ciberseguridad o los datos?**

Sí **No**

a. En caso afirmativo, proporcione detalles adicionales:

Preguntas complementarias - complete estas secciones sólo si aplican a su negocio

Información Biométrica

1. **Recopila información biométrica de:**

a. Empleados	**Sí**	**No**
b. Proveedores de Servicios o Contratistas	**Sí**	**No**
c. Clientes	**Sí**	**No**
d. Otros (por favor especifique)	**Sí**	**No**

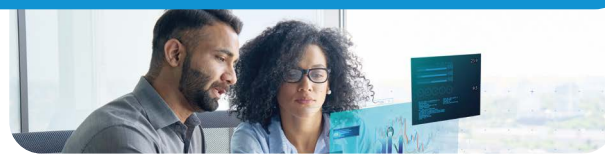
2. **Con respecto a los datos biométricos recopilados, utilizados o almacenados de los empleados:**
   a. ¿Obtiene el consentimiento por escrito y una autorización de cada individuo? **Sí** **No**
   b. ¿Requiere que cada empleado firme un acuerdo de arbitraje con renuncia a acciones colectivas? **Sí** **No**
3. **¿Cuenta con políticas escritas formales acerca de los requisitos de privacidad de la información biométrica que aborden claramente las directrices de conservación y destrucción?** **Sí** **No**
4. **¿Se obtiene siempre el consentimiento por escrito y es éste explícito?**
5. **¿Cuándo empezó a recopilar, almacenar o procesar datos biométricos?**
6. **¿Desde cuándo se exige el consentimiento explícito por escrito?**
7. **Por favor, detalle la cantidad de registros de información biométrica que posee o de la que es responsable:**

Tecnología Operativa

En este apartado, la tecnología operativa (TO) se diferencia de la tecnología de la información (IT) en que la OT se centra en la vigilancia, la gestión y el control de las operaciones industriales o los equipos físicos, mientras que la IT se centra en el intercambio, el procesamiento y el almacenamiento de datos electrónicos. La tecnología operativa puede incluir Sistemas de Control Industrial (ICS), Control de Supervisión y Adquisición de Datos (SCADA), Controladores Lógicos Programables (PLC), Sistemas de Control Distribuido (DCS), sistemas de robótica, etc.

1. **¿Cuenta con una política formal de seguridad TO que incluya la seguridad cibernética?** **Sí** **No**
2. **¿Quién es el responsable de implementar y mantener la seguridad cibernética de los sistemas y redes TO?**
   - Organización de seguridad de TI
   - Ingeniería o unidad de negocio
   - Otro
3. **¿Cuántos centros de producción tiene?**
   a. Qué porcentaje son: operado por usted **%** operado por un proveedor **%**
4. **¿Los centros de producción están segmentados entre sí para minimizar la posibilidad de que varios centros se vean afectados por el mismo evento o incidente?**

Sí **No**



NIT 860.037.013-6
Calle 33 # 6B - 24, pisos 1, 2 y 3
Tel: (601) 327 4712 / 13
Bogotá D.C. - Colombia
Somos Grandes Contribuyentes
IVA Régimen Común - Autorretenedores

5. **¿Cómo se separan los activos y redes de tecnología de la información de los de TO?**
   - ○ VLAN
   - ○ Diodo de datos
   - ○ Configuración de firewalls (lista de control de acceso)
   - ○ Air-gap
   - ○ Firewalls basados en host
   - ○ TO con acceso restringido a Internet
   - ○ Zonas desmilitarizadas (DMZ)
   - ○ Controles de acceso de menor privilegio
   - ○ Otro

6. **¿Permite el acceso remoto a los entornos de TO?** **Sí** ○ **No** ○

   En caso afirmativo, complete lo siguiente:

   a. ¿Cómo protege el acceso remoto a la TO? (seleccione todo lo que corresponda)
   - ○ VPN (Red Privada Virtual)
   - ○ Autenticación de Múltiples Factores
   - ○ SSO (Single Sign-on) vía MFA
   - ○ Acceso de Confianza Cero a la Red (ZTNA)
   - ○ Cifrado de tráfico
   - ○ Otro

   Por favor, detalle cualquier excepción a lo anterior, o proporcione comentarios adicionales:

7. **Por favor, describa su proceso de gestión de parches y cadencia para las TO:**

8. **¿Supervisa y responde a los eventos que se producen en su entorno TO de la misma manera que lo hace en su entorno de tecnologías de la información?** **Sí** ○ **No** ○

9. **¿Mantiene y prueba las copias de seguridad de su entorno de TO?** **Sí** ○ **No** ○

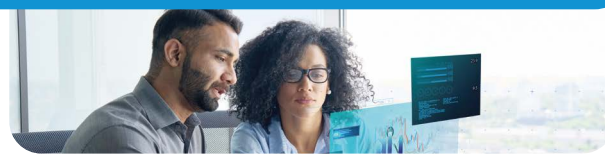
   a. En caso afirmativo, ¿cómo se protegen estas copias de seguridad? (seleccione todo lo que corresponda):
   - ○ Tecnología de copia de seguridad inmutable o de Escritura Única y Lectura Múltiple (WORM)
   - ○ Copias de seguridad completamente Offline / Air-gapped (cinta / discos no montados) desconectadas del resto de su red
   - ○ Acceso restringido a través de una Cuenta Privilegiada separada que no está conectada al Directorio Activo u otros dominios
   - ○ Acceso restringido a las copias de seguridad mediante MFA
   - ○ Cifrado de las copias de seguridad
   - ○ Las copias de seguridad de TO están segmentadas de las redes de TI
   - ○ Ninguna de las anteriores
   - ○ Otro

10. **Por favor, describa su capacidad de recurrir a procedimientos manuales o de otro tipo para solucionar problemas si los sistemas se ven afectados por un incidente cibernético:**

Adquisiciones

1. **¿Cuántas adquisiciones ha realizado en los últimos tres años?**

2. **Detalle el nombre de las entidades adquiridas, el tamaño de las mismas y las fechas de las adquisiciones:**



NIT 860.037.013-6
Calle 33 # 6B - 24, pisos 1, 2 y 3
Tel: (601) 327 4712 / 13
Bogotá D.C. - Colombia
Somos Grandes Contribuyentes
IVA Régimen Común - Autorretenedores

3. **¿Cuándo auditan y evalúan la postura y la exposición de seguridad cibernética de dichas entidades?**
   - Antes de la adquisición
   - Después de la adquisición, pero antes de la integración
   - Las evaluaciones de ciberseguridad rara vez se realizan antes o después de la adquisición
   - Otro
4. **Por favor, detalle la estrategia de integración, los plazos y la debida diligencia realizada en relación con las entidades adquiridas:**

Servicios profesionales

1. **¿Contrata algún tipo de seguro de responsabilidad civil profesional?** **Sí** **No**
2. **En caso afirmativo, ¿contiene su póliza alguna exclusión relativa a riesgos cibernéticos?** **Sí** **No**
3. **¿Opera, gestiona o aloja algún sistema tecnológico en apoyo de sus servicios profesionales?** **Sí** **No**
   a. ¿Los datos y sistemas relacionados con estos servicios son responsabilidad de su cliente? **Sí** **No**
   Por favor, especifique:

   b. Si aloja datos y sistemas para sus clientes, ¿se aplican los controles descritos en este formulario de propuesta a estos sistemas alojados en relación con la resiliencia, las estrategias de copia de seguridad y el cumplimiento de la privacidad de los datos? **Sí** **No**
   Comentario adicional:

Comercio al por menor u operaciones de venta al detal

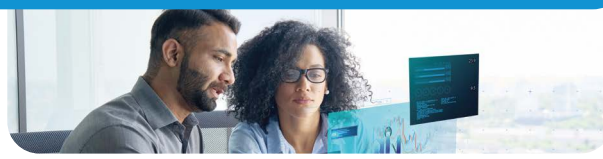
1. **¿Segrega sus equipos y redes de punto de venta o de procesamiento de transacciones de otras redes de TI?** **Sí** **No**
2. **Por favor, describa su proceso de gestión de parches y cadencia para las aplicaciones de software de punto de venta:**
3. **¿Qué porcentaje de sus puntos de venta y/o terminales de pago son compatibles con la tecnología de chip que cumple con las normas EMV?** **%**
4. **Por favor, indique el nombre del proveedor o proveedores en los que se apoya para el procesamiento de los pagos:**
5. **¿Están los sistemas de punto de venta protegidos por antimalware y supervisados por sus recursos de seguridad de la información?** **Sí** **No**
   Comentario adicional:
6. **¿Tienen locales franquiciados o acuerdos de franquicia?** **Sí** **No**
   a. En caso afirmativo, proporcione más información sobre quién es responsable de la seguridad cibernética en las franquicias y cómo se aplican los controles de seguridad cibernética de forma consistente:

Controles Planificados (opcional)

Por favor detalle que mejoras tiene planificados para los próximos 12 meses con relación a la gestión de riesgos cibernéticos o seguridad de la información y los datos

seguros mundial®

PRODUCTO CYBER EMPRESARIAL
FORMULARIO DE RANSOMWARE



NIT 860.037.013-6
Calle 33 # 6B - 24, pisos 1, 2 y 3
Tel: (601) 327 4712 / 13
Bogotá D.C. - Colombia
Somos Grandes Contribuyentes
IVA Régimen Común - Autorretenedores

Coberturas

1. Por favor, facilite detalles de sus pólizas de seguro actuales (si aplica)

Cobertura – marque si tiene una póliza en vigor tiene una póliza en vigor	Límite	Deducible	Asegurador	Fecha de vencimiento (DD/MM/AAAA)
Riesgos Cibernéticos				/ /
Crime				/ /
Responsabilidad Civil Profesional				/ /

Declaraciones

Este formulario de propuesta debe estar firmado y fechado antes de su envío. Si se celebra el contrato de seguro, esta declaración se adjuntará al mismo.

Declaro que, la Compañía Mundial S.A. identificada con NIT: 860.037.013-6 en su calidad de Responsable de Tratamiento de Datos Personales me han informado: 1) Que la Política de Tratamiento de Datos Personales se encuentran en la página web http://www.segurosmundial.com.co/proteccion-de-datos/ 2) Que son facultativas las respuestas a las preguntas sobre datos de niñas, niños, adolescentes y aquellas que versen sobre datos sensibles y en consecuencia no he sido obligado a responderlas; 3) Que como titular de la información, me asisten los derechos previstos en las leyes 1266 de 2088 y 1581 de 2012, en especial me asiste el derecho a conocer, actualizar, rectificar, revocar y suprimir mis datos personales.

Autorizo de manera previa, expresa e informada a la Compañía Mundial S.A. y/o cualquier sociedad controlada, directa o indirectamente, que tengan participación accionaria o sean asociados, domiciliadas en Colombia y/o en el exterior, terceros contratados por esta o a quien la represente, en adelante **LA COMPAÑÍA** para que realice el tratamiento de mis datos personales para las siguientes finalidades:

(i) Tramitar mi solicitud de vinculación como consumidor financiero, usuario, cliente o cliente potencial; **(ii)** Negociar, celebrar y ejecutar el contrato de seguro; **(iii)** Ejecutar y cumplir los contratos que celebre **LA COMPAÑÍA** con entidades en Colombia o en el extranjero para cumplir con su objeto social; **(iv)** El control y prevención de fraude, lavado de activos, financiación del terrorismo, financiación de la proliferación de armas de destrucción masiva, soborno o corrupción; **(v)** Controlar el cumplimiento de requisitos relacionados con el Sistema de Seguridad Social Integral; **(vi)** Ejecutar acciones, investigaciones y estudios de perfilamiento comercial, técnico, estadístico, actuarial, de analítica, de tendencias de mercado, inteligencia de negocios, hábitos de consumo, definición de patrones; inteligencia artificial; encuestas de satisfacción en la experiencia de cliente; **(vii)** Enviar información sobre los productos, servicios, eventos, actividades de índole comercial, alianzas y publicidad de LA COMPAÑÍA, a través de los medios físicos o virtuales registrados; **(viii)** Consultar, almacenar, administrar, transferir, procesar y reportar mi comportamiento financiero a los Operadores de la Información; **(ix)** Transferir o transmitir los datos personales a terceros contratados ubicados en el territorio nacional o en el extranjero, en cumplimiento de obligaciones legales y/o contractuales;**(x)** Recolectar, almacenar, actualizar, usar, y conservar mis datos personales sensibles, tales como, datos sobre mi estado de salud, que sean indispensables para la prestación del servicio contratado con **LA COMPAÑÍA**, en caso de que aplique; **(xi)** Recolectar, almacenar, actualizar, usar, y conservar los datos personales de mis hijos o representados menores de edad, en calidad de su representante legal o tutor, que sean indispensables para la prestación del servicio contratado con **LA COMPAÑÍA**, en caso de que aplique; **(xii)** Acceder a consultar, solicitar, suministrar, reportar, procesar, usar, y en general dar un tratamiento a toda la información contenida en mi historia laboral del RAIS (Régimen de Ahorro individual con Solidaridad) por las veces que se requiera, y a la información que se encuentre administrada por la Asociación Colombiana de Administradoras Fondos de Pensiones (Asofondos de Colombia) y por las Administradoras de Fondos de Pensiones en las que he estado vinculado; **(xiii)** Tramitar y gestionar felicitaciones, solicitudes, peticiones o quejas o requerimientos de autoridades en ejercicio de sus funciones; **(vix)** Las demás finalidades que se determinen con base a la ejecución de los procesos de Seguros Mundial, en todo caso que estén acorde a la Ley.

LA COMPAÑÍA conservará mis datos personales mientras sea necesario para el cumplimiento de cualquier obligación legal y contractual o para la atención de cualquier queja o reclamo judicial o extrajudicial.

Autorizo de manera previa, expresa e informada a **LA COMPAÑÍA** para tratar mis datos personales para las finalidades anteriormente descritas: Sí ○ No ○

Autorizo recibir comunicaciones comerciales y publicitarias personalizadas de **LA COMPAÑÍA** a través de sus canales autorizados: Sí ○ No ○

Con la firma del presente documento autorizo a **LA COMPAÑÍA** a realizar gestión de cobranza en caso de que así se requiera, por los siguientes canales: llamada telefónica, correo electrónico, SMS o WhatsApp.

En caso de no autorizar el contacto por alguno de los canales anteriormente mencionados, por favor especifique cuál desea excluir.

Declaro que la totalidad de la información suministrada en este formulario es exacta, y que no se ha omitido voluntariamente, ni siquiera suprimido ningún hecho. También informaré al Asegurador cualquier modificación que ocurra desde este día hasta la fecha de inicio de vigencia de la póliza de seguro.

La tergiversación o no divulgación de cualquier hecho material por parte del solicitante del seguro hará que cualquier póliza emitida sea nula y eximirá a Seguros Mundial de toda responsabilidad en la materia.

Manifiesto que las declaraciones y los detalles hechos en este Formulario son ciertos y que no he expresado incorrectamente ni suprimido ningún hecho material.

Acepto que en caso de que haya algún cambio sustancial en las declaraciones hechas aquí antes de la fecha de entrada fecha de inicio de vigencia de la póliza, notificaré a Seguros Mundial y las cotizaciones pendientes pueden ser modificadas y/o retiradas.

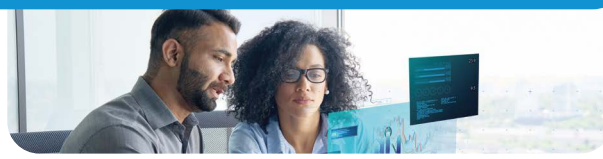
El presente formulario deberá ser firmado por un representante autorizado del Solicitante del seguro

Declaro que la totalidad de la información suministrada en este formulario es exacta, y que no se ha omitido voluntariamente, ni siquiera suprimido ningún hecho. También informaré al Asegurador cualquier modificación que ocurra desde este día hasta la fecha de inicio de vigencia de la póliza de seguro.

seguros mundial®

PRODUCTO CYBER EMPRESARIAL
FORMULARIO DE RANSOMWARE

NIT 860.037.013-6
Calle 33 # 6B - 24, pisos 1, 2 y 3
Tel: (601) 327 4712 / 13
Bogotá D.C. - Colombia
Somos Grandes Contribuyentes
IVA Régimen Común - Autorretenedores



Firma

El presente formulario deberá ser firmado por un representante autorizado del Solicitante del seguro.

Firma	Nombre	Fecha	Cargo

Definiciones

Acceso de Confianza Cero a la Red (ZTNA): Es un servicio que implica la creación de un límite de acceso lógico basado en una identidad y contexto en torno a una aplicación o conjunto de aplicaciones.

Agente de Seguridad de Acceso a la Nube (CASB): Es un software que supervisa la actividad entre los usuarios de los servicios en la nube y las aplicaciones en la nube para hacer cumplir las políticas de seguridad y evitar la actividad maliciosa.

Aislamiento y Contención de Aplicaciones: Esta tecnología puede bloquear, restringir o aislar puntos finales específicos para que no realicen acciones potencialmente dañinas entre los puntos finales y otras aplicaciones o recursos con el objetivo de limitar el impacto de un sistema o punto final comprometido.

Análisis Heurístico: Más allá de la detección tradicional basada en firmas del software antivirus básico, el Análisis Heurístico busca propiedades sospechosas en el código, y puede determinar la susceptibilidad de un sistema hacia una amenaza particular utilizando varias reglas de decisión o métodos de ponderación diseñados para detectar virus informáticos previamente desconocidos, así como nuevas variantes de virus ya existentes.

Autenticación de Múltiples Factores (MFA): La MFA es un método de autenticación electrónica utilizado para garantizar que sólo las personas autorizadas tengan acceso a sistemas o datos específicos. El usuario debe presentar dos o más factores: 1) algo que sabe, 2) algo que tiene, o 3) algo que usted es. Algo que sabe puede incluir su contraseña o un código PIN. Algo que tiene puede incluir un dispositivo físico como un ordenador portátil, un dispositivo móvil que genera un código único o recibe una llamada de voz o un mensaje de texto, un token de seguridad (memoria USB o token de hardware), o un certificado o token único en otro dispositivo. Algo que usted es puede incluir identificadores biométricos.

Tenga en cuenta que los siguientes no son segundos factores aceptables: una clave secreta compartida, una dirección IP o MAC, una VPN, un procedimiento de re-autenticación mensual o la autenticación VOIP.

Base de Datos de Gestión de la Configuración (CMDB): Es una base de datos que se usa para almacenar información sobre los activos de hardware y software de una organización, y normalmente se utiliza para identificar y administrar la configuración y la relación entre los activos

Centro de Operaciones de Seguridad (SOC): Es una función centralizada que incluye personas, procesos y tecnología diseñados para supervisar, detectar, prevenir, analizar y responder continuamente a los incidentes de seguridad cibernética.

Cifrado: Es el método de conversión de datos de un formato legible a un formato codificado. Sólo puede volver a ser legible con la clave para quitar el cifrado asociada.

Common Vulnerability Scoring System (CVSS): Es una valoración estándar abierta de la industria sobre la gravedad de las vulnerabilidades, que asigna puntuaciones en función de la facilidad y el impacto potencial de la explotación de estas.

Correo identificado con claves de dominio (DKIM): Es un método estándar de autenticación del correo electrónico que añade una firma digital a los mensajes salientes para permitir una mejor verificación del remitente.

Cuentas Privilegiadas: Se refiere a las cuentas que proporcionan niveles de acceso administrativos o especializados basados en un nivel de permiso superior.

Dispositivos Gestionados: Es un dispositivo que requiere un agente gestor o una herramienta de software que permita a los equipos de tecnología de la información controlar, supervisar y asegurar dicho dispositivo. Un dispositivo no gestionado sería cualquier dispositivo que no pueda ser visto o gestionado por dichos productos o equipos tecnológicos

Dominio de Directorio Activo: Un dominio de Directorio Activo es una colección de objetos dentro de una red de Directorio Activo de Microsoft. Un objeto puede ser un solo usuario o un grupo, o puede ser un componente de hardware, como un computador o una impresora. Cada dominio tiene una base de datos que contiene información sobre la identidad de los objetos.

Endpoint Detection and Response (EDR): Es una solución que registra y almacena los comportamientos a nivel de sistema de los puntos finales, utiliza diversas técnicas de análisis de datos para detectar comportamientos sospechosos del sistema, proporciona información contextual, bloquea la actividad maliciosa y ofrece sugerencias de reparación para restaurar los sistemas afectados.

Escritura Única y Lectura Múltiple (WORM): Es un dispositivo de almacenamiento de datos en el que la información, una vez escrita, no puede modificarse.

Estaciones de Trabajo con Acceso Privilegiado: Es una estación de trabajo reforzada configurada con controles y políticas de seguridad que restringen el acceso administrativo local y las herramientas de productividad para minimizar la superficie de ataque a sólo lo que es absolutamente necesario para realizar las tareas sensibles del trabajo. Estas estaciones de trabajo no suelen tener acceso al correo electrónico ni a la navegación general por la web.

Evento de falla del sistema: Es la interrupción involuntaria, el apagón, la perturbación, la inaccesibilidad o el mal funcionamiento de los sistemas informáticos o de los programas informáticos causados por medios no malintencionados. Un evento de fallo del sistema puede ser causado por un corte de energía, un error humano u otra interrupción.

Extended Detection and Response (XDR): Es una herramienta de detección de amenazas de seguridad y respuesta a incidentes que integra de forma nativa varios productos de seguridad en un sistema de operaciones de seguridad cohesionado que unifica todos los componentes con licencia, que suelen incluir puntos finales, redes, servidores, servicios en la nube y SIEM, entre otros.

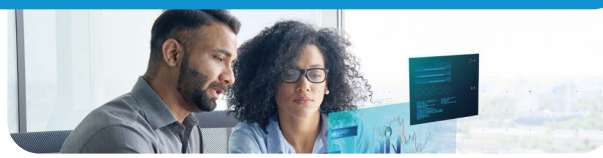
Filtrado de URL o Filtrado Web: Es la tecnología que restringe los sitios web que un usuario o navegador puede visitar en su computador, normalmente filtrando los s sitios web maliciosos o vulnerables conocidos.

Firewall de Aplicaciones Web (WAF): Es un tipo de firewall de red, de host o basado en la nube que se coloca entre una aplicación e Internet, para protegerla contra el tráfico malicioso y otros ataques web comunes que suelen tener como objetivo los datos sensibles de las aplicaciones.

Gestión de Accesos Privilegiados (PAM): Describe los procesos y la tecnología de una empresa que soporta las cuentas privilegiadas. Las soluciones PAM ofrecen una capa adicional de protección, y suelen tener una gestión automatizada de contraseñas, capacidades de aplicación de políticas, capacidades de gestión del ciclo de vida de las cuentas, así como supervisión y elaboración de informes sobre la actividad de las cuentas privilegiadas.

Gestión de Dispositivos Móviles (MDM): Es un software que se instala en un dispositivo gestionado y que permite a los administradores de tecnologías de la información controlar, supervisar y proteger los puntos finales de los dispositivos móviles.

NIT 860.037.013-6
Calle 33 # 6B - 24, pisos 1, 2 y 3
Tel: (601) 327 4712 / 13
Bogotá D.C. - Colombia
Somos Grandes Contribuyentes
IVA Régimen Común - Autorretenedores



Gestión de Eventos e Información de Seguridad (SIEM): Es la tecnología y los servicios relacionados que proporcionan un análisis en tiempo real de las alertas de seguridad cibernética procedentes de un conjunto de fuentes, incluidos los puntos finales y las aplicaciones, para permitir una mejor detección, el cumplimiento de la normativa y la gestión de incidentes.

Gestión de Identidades y Control de Acceso (IAM): garantiza que los usuarios correctos tengan el acceso adecuado a los recursos tecnológicos, e incluye la gestión de los nombres de usuario, las contraseñas y los privilegios de acceso a los sistemas y la información

Incidente Cibernético: Incluye el acceso no autorizado a sus sistemas informáticos, la piratería informática, el malware, el virus, el ransomware, el ataque de denegación de servicio distribuido, el uso indebido interno de información privilegiada, el error humano o de programación, la interrupción del sistema o cualquier otro evento cibernético relacionado.

Información de Identificación Personal (IIP): Significa cualquier dato que pueda ser usado para identificar a un individuo específico. Esto puede incluir registros médicos o de salud de empleados o clientes, números de identificación emitidos por el gobierno, nombres de usuario de inicio de sesión, direcciones de correo electrónico, números de tarjetas de crédito, información biométrica y otra información personal relacionada.

Inteligencia de Amenazas: Es la información sobre las amenazas actuales a la seguridad, las vulnerabilidades, los objetivos, los actores maliciosos y sus implicaciones que pueden utilizarse para tomar decisiones en materia de seguridad.

Leyes y Normas de Privacidad: El conjunto de leyes que establecen los requisitos y regulaciones para la recopilación, el almacenamiento y el uso de la información personal identificable, la información persona de salud, la información financiera de los individuos y otros datos sensibles que pueden ser detectados por organizaciones públicas o privadas, u otros individuos.

Managed Detection and Response (MDR): Es un servicio de ciberseguridad gestionado que proporciona detección de intrusiones de malware y actividad maliciosa en su red, y asiste en la respuesta rápida a incidentes para eliminar esas amenazas con acciones sucintas de remediación.

Microsegmentación: Es una técnica de seguridad de la red que permite a los arquitectos de seguridad dividir lógicamente el centro de datos en distintos segmentos de seguridad hasta el nivel de carga de trabajo individual, y luego definir los controles de seguridad y ofrecer servicios para cada segmento único.

Offline or Air-gapped: En lo que respecta a las soluciones de copia de seguridad, el almacenamiento offline o air-gapped significa que una copia de sus datos y configuraciones se almacena en un entorno desconectado e independiente del resto de su red. Las copias de seguridad en cinta física o en disco no montado que no están conectadas a Internet o a la red LAN se considerarían fuera de línea.

Orquestación, Automatización y Respuesta de Seguridad (SOAR): Es una tecnología utilizada para racionalizar y priorizar automáticamente las alertas de seguridad cibernética procedentes de un conjunto de fuentes, incluidos los puntos finales y las aplicaciones (similar a una solución de Gestión de Eventos e Información de Seguridad), pero ofrece una respuesta automatizada mejorada y técnicas de predicción mejoradas.

PCI DSS: PCI DSS son las siglas de Payment Card Industry Data Security Standard. Define los requisitos que debe cumplir una empresa si maneja información de tarjetas de pago o acepta transacciones con tarjetas de pago.

Perímetro de Servicio de Acceso Seguro (SASE): es un servicio en la nube que combina funciones de red y seguridad basadas en la nube, como SWG, CASB y ZTNA, con capacidades WAN.

Plataforma Centralizada de Protección de Endpoints: es una solución que se despliega en los dispositivos de punto final (endpoint) para prevenir los ataques de malware basados en archivos, detectar la actividad maliciosa y proporcionar las capacidades de investigación y reparación necesarias para responder a los incidentes y alertas de seguridad dinámicas

Protección Avanzada de Endpoints : Protección Avanzada de Endpoints es un dispositivo o software que proporciona protección y monitorización de los puntos finales (endpoints) de su red. Los puntos finales incluyen computadores de escritorio y portátiles, tabletas, teléfonos móviles, servidores y cualquier otro dispositivo conectado a su red.

Protección del Sistema de Nombres de Dominio: Es un servicio que impide el acceso a los dominios que se sabe que son maliciosos, y también permite realizar análisis adicionales y alertas sobre las solicitudes de dominios bloqueados.

Protocolo de Escritorio Remoto (RDP): Es un protocolo de Microsoft que permite el uso remoto de un computador de escritorio. Sin protecciones adicionales, RDP tiene algunas vulnerabilidades de seguridad graves.

Reclamación por Contenidos Electrónicos: Incluye cualquier reclamación por desprestigio del producto, calumnia, difamación comercial, publicidad denigratoria, plagio o similares de su sitio web o cuentas de redes sociales.

Sandboxing: En relación con las soluciones de correo electrónico, un sandbox filtra los mensajes de correo electrónico con enlaces URL desconocidos, archivos adjuntos u otros archivos, lo que permite probarlos en un entorno separado y seguro antes de permitir que pasen a su red o servidores de correo.

Sender Policy Framework (SPF): Es un método de autenticación de correo electrónico que se utiliza para evitar que personas no autorizadas envíen mensajes de correo electrónico desde su dominio y, en general, ayuda a proteger a los usuarios y destinatarios de correo electrónico contra el spam y otros mensajes potencialmente peligrosos.

Single Sign On (SSO): Es un método de autenticación que permite a los usuarios autenticarse de forma segura en varias aplicaciones y sitios web sin tener que iniciar sesión en cada uno de ellos. Para ello se establece una relación de confianza entre una aplicación, conocida como proveedor de servicios, y un proveedor de identidad.

Sistema de Detección de Intrusos (IDS): Es un dispositivo o software que supervisa su red en busca de actividades maliciosas o violaciones de las políticas.

Soluciones Empresariales o Integradas de Prevención de Pérdida de Datos (DLP): Son productos de software y reglas centradas en la prevención de la pérdida de, el acceso no autorizado a, o el uso indebido de. información sensible o crítica. La DLP empresarial describe las soluciones dedicadas implantadas en toda una organización y puede incluir alertas, cifrado, supervisión y otros controles de movimiento y prevención para los datos en reposo y en movimiento. La DLP integrada utiliza los servicios y complementos de las herramientas de seguridad existentes para lograr el mismo objetivo de prevenir la pérdida y el uso indebido de los datos.

Violación de datos: Se trata de un incidente en el que una parte no autorizada ha tomado, perdido o visto información personal sensible o información corporativa confidencial.