

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

V2
DURACIÓN: 40 MINUTOS

SONIDO	IMÁGENES	LOCUCIÓN
Sonido de cortinilla.	[Cortinilla con el título:] Curso Anual de Riesgos SURA Asset Management	[Segmento 1. Introducción y Sistema de Control Interno SURA AM] (Introducción)
Música dinámica, de apertura de programa.	Set virtual moderno. Conductor a cuadro, que se expresará en todo momento con actitud dinámica y jovial.	Conductor: ¡Hola, qué tal! ¡Le mando un afectuoso saludo a toda la increíble familia de SURA Asset Management en Latinoamérica! Estoy muy contento de estar aquí para hablar de un tema fundamental que nos concierne a todos: los riesgos a los que se enfrenta nuestra organización. A lo largo de este curso, vamos a conocer los diferentes tipos de riesgos y, lo más importante, las estrategias para gestionarlos. La idea es revisar los distintos planes de acción para proteger a la compañía ¡y así lograr que siga creciendo de manera sostenible y continúe aportando valor a la sociedad! Descubriremos que en la gestión de riesgos, ¡todos cumplimos un papel fundamental! ¿Estás listo? ¡Comenzamos!
Música que indique cambio de tema.	Gráficos digitales dinámicos que reflejen modernidad.	
Música dinámica y jovial de fondo.	[Texto en pantalla:] Sistema de Control Interno Un campo de futbol con una cancha dividida en tres zonas, representando las líneas de defensa del SCI.	(Sistema de Control Interno) Conductor: Vamos a empezar con algo esencial: el Sistema de Control Interno de SURA Asset Management . Imaginémoslo como el esquema táctico de un equipo de futbol, que nos permite estar siempre enfocados en nuestros objetivos, ser efectivos en la operación, cumplir las reglas y ser súper transparentes al preparar nuestros reportes financieros.

Dio formato: Inglés (Estados Unidos)

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	Una pizarra donde aparecen los tres conceptos clave: Autocontrol Autorregulación Autogestión	Y en el equipo de SURA AM, todos los jugadores, desde la Alta Dirección hasta cada uno de los colaboradores, tienen un papel vital en esta estrategia. ¡Nadie se queda en la banca! Siguiendo con la analogía del futbol, para ganar el campeonato, hay tres principios básicos: 1. Autocontrol: Se refiere a que cada jugador debe evaluar su desempeño, corregir errores y asegurarse de cumplir con sus funciones para alcanzar los objetivos establecidos por la Dirección. 2. Autorregulación: Consiste en seguir las reglas del juego al aplicar métodos, normas, políticas y procedimientos para optimizar el Sistema de Control Interno. 3. Autogestión: Se refiere a actuar con inteligencia y tomar decisiones efectivas, para asegurar que el Sistema de Control Interno funcione como se espera: con eficacia y al más alto nivel.
Música dinámica y jovial de fondo.	Una animación que muestra una alineación de futbol con tres líneas de jugadores, que se van enfocando conforme se habla de cada línea. [Texto en pantalla:] Modelo de 3 líneas [Texto en pantalla:] Primera línea de defensa: Colaboradores y dueños de los procesos [Texto en pantalla:] Segunda línea de defensa: Áreas de Riesgo y Cumplimiento	Ahora hablemos del esquema de prevención de riesgos, que conocemos como el Modelo de 3 Líneas de Defensa: La primera línea cumple un papel similar al de los delanteros y los volantes; y corresponde a la labor de los colaboradores y dueños de los procesos. Ellos se encargan de identificar los riesgos, crear las estrategias para evitarlos y asegurarse de que todo funcione con los recursos necesarios. En otras palabras, hacen todo lo posible para impedir que el balón llegue a la siguiente línea de defensa. La segunda línea está a cargo de las áreas de Riesgo y Cumplimiento, quienes actúan como los medios de contención y defensas. Ellos nos brindan las metodologías y acompañan a la

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	[Texto en pantalla:] Tercera línea de defensa: Auditoría	primera línea para prevenir riesgos. Monitorean el cumplimiento de las políticas y reportan posibles riesgos críticos y altos, para contenerlos y evitar que lleguen a la última línea de defensa. La tercera y última línea de defensa entra en acción cuando las dos anteriores han sido superadas y debe activarse el último filtro de seguridad. ¡Es como nuestro portero! Cuando el oponente llega hasta este punto, quiere decir que las otras dos líneas han fallado y estamos en una situación vulnerable. La última línea es el área de Auditoría, que evalúa los controles implementados, emite recomendaciones relacionadas con el Sistema de Control Interno y reporta si ha detectado riesgos.
Música dinámica y jovial de fondo.	[Texto en pantalla:] Solución attento Esquema de attento (página 4 del documento base), que se va armando como un rompecabezas hasta formar un escudo que en medio diga “attento”.	Pero justamente para evitar que el oponente se acerque a nuestra área y anote gol, ¡contamos con una solución de clase mundial! Se llama attento y nos permite: • Contar con un repositorio centralizado de riesgos y las medidas para tratarlos. • Mantener actualizados los procesos y generar reportes automáticos, para que puedan consultarse en línea. • Dar seguimiento a los planes de acción para atender los posibles puntos débiles del Sistema de Control Interno. • Reportar los eventos de riesgo y dar seguimiento a su gestión. • Asegurar el cumplimiento de normativas. • E identificar los procesos críticos para asegurar la continuidad del negocio. Básicamente, es como nuestro VAR: nos permite analizar las jugadas en tiempo real y tomar las mejores decisiones para evitar cualquier sorpresa en el partido.

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música inspiradora.	Un estadio lleno de energía, con el logo de la compañía en la pantalla central.	Y bueno, para cerrar, te diría que para que seamos un equipo ganador necesitamos jugar con una estrategia clara. Con el Sistema de Control Interno de SURA Asset Management, ¡sabemos cómo defendernos de los riesgos!
Música de cierre de segmento.	Conductor se despide.	Y atento nos permite estar siempre preparados. Así que, ¡juguemos siempre para ganar! Con esto concluimos este segmento. ¡Te veo en el siguiente!
Sonido cortinilla.	[Cortinilla:] Riesgo operacional Ley Sarbanes-Oxley	[Segmento 2. Riesgo operacional / SOX] (Riesgo operacional)
Música dinámica de inicio de segmento.	Desaparece “Ley Sarbanes-Oxley” para indicar que comenzaremos con “Riesgo Operacional” Conductor sonriente a cuadro.	Conductor: ¡Hola, hola! ¡Bienvenido a este segmento!, donde comenzaremos platicando sobre el riesgo operacional . Explicaremos qué es, cómo lo gestionamos en SURA Asset Management y por qué es tan crucial para cumplir nuestros objetivos estratégicos. ¡Acompáñame que ya comenzamos!
Música dinámica y jovial de fondo.	[Texto en pantalla:] ¿Qué es un riesgo?	Ok, para arrancar, vamos con un concepto básico: ¿qué es un riesgo? En palabras sencillas, es cualquier situación que podría afectar o impedir que la empresa cumpla sus objetivos.
	Gráfica de barras con una flecha que indica descenso. [Texto en pantalla:] Riesgo operacional Íconos de personas, engranes, computadoras, edificios, un rayo.	Ahora bien, el riesgo operacional es el que surge por fallas en personas, procesos, tecnología, infraestructura ¡o hasta por situaciones externas que pueden salirse de nuestras manos! El riesgo operacional involucra los riesgos legales y reputacionales .
	El conductor señala un gráfico flotante en 3D que divide el	Y claro, todas las compañías asumen riesgos, pero ¿cómo sabemos si estamos tomando un

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	espacio en dos: “Apetito de riesgo” a la izquierda y “Perfil de Riesgo” a la derecha. Ícono de una mano con el pulgar hacia arriba. Semáforo indicando riesgos altos, medios y bajos.	riesgo que realmente vale la pena? Esto lo definimos mediante dos conceptos clave: el apetito de riesgo y el perfil de riesgo. El apetito de riesgo es cuando definimos qué tipo de riesgo estamos dispuestos a asumir como compañía para cumplir nuestros objetivos estratégicos. Por su parte, el perfil de riesgo es el panorama de todos los riesgos que enfrentamos. Aquí evaluamos qué tan expuestos estamos y cómo podemos gestionarlos.
Música dinámica y jovial de fondo.	[Texto en pantalla:] Tipos de riesgo Operacionales Ícono de personas y computadoras. Legales Ícono de martillo de un juez. Reputacionales Ícono de reporteros. Financieros Ícono de gráfica de resultados financieros. Estratégicos Ícono de ejecutivos.	En SURA Asset Management identificamos varios tipos de riesgo, como los siguientes: • Operacionales, que, como ya dijimos, incluyen fallas en personas, procesos, tecnología, infraestructura o eventos externos. • Legales, que se producen cuando se incumplen regulaciones y políticas por actos antiéticos. • Reputacionales, que ocasionan daños en el prestigio de la organización. • Financieros, que afectan la rentabilidad del negocio. • Y estratégicos, que generan desviaciones en el crecimiento o el valor para los accionistas.
Música dinámica y jovial de fondo.	[Texto en pantalla:] Factores de riesgos: Internos Gráficos de computadoras. Externos Un huracán.	Además, los factores de riesgo se dividen en internos y externos. Los internos son los que tienen que ver con los recursos humanos, los procesos, la tecnología y la infraestructura; mientras que los externos están relacionados con fenómenos naturales o actos de terceros.
	[Texto en pantalla:] Tipos de riesgo operacional	Ahora hablemos de los tipos de riesgo operacional. Estos pueden ser:

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	Fraude interno Íconos de tarjetas de crédito, internet, huellas digitales, passwords. Fraude externo Símbolo de: ¡Peligro! Relación y seguridad laboral Ícono de empleados. Daños a activos físicos Edificios. Fallas tecnológicas Computadoras. Errores en procesos Símbolo de "error". Malas prácticas empresariales Ícono de ejecutivos y clientes.	• El fraude interno, es decir, cuando un empleado o un tercero contratado intenta defraudar o apropiarse indebidamente de activos, o incumple normas o leyes. • El fraude externo, cuando el problema viene de afuera, de personas o entidades ajenas a la empresa. • Los riesgos derivados de incumplir leyes laborales. • Los daños a los activos físicos, causados por desastres naturales, o actos de terrorismo o vandalismo. • Las fallas tecnológicas, que es cuando hay problemas con el hardware, software o las telecomunicaciones, que pueden comprometer la seguridad de la información. • Los errores en la ejecución de procesos que afecten la relación con socios comerciales o proveedores. • O malas prácticas empresariales, ya sea involuntarias o negligentes, que afectan a nuestros clientes.
Música dinámica y jovial de fondo.	[Texto en pantalla:] ¿Cómo se gestionan esos riesgos? Identificar Animación de una lupa, como buscando un riesgo en una lista. Medir	A continuación toca responder: ¿cómo se gestionan esos riesgos? • Primero, identificamos el tipo de riesgo, lo cual implica reconocerlo y describirlo adecuadamente. Esto lo hacemos a través de auditorías, controles externos, consultorías o incluso cuando ya estamos enfrentando un incidente. • Después, medimos el riesgo. Aquí respondemos dos preguntas: ¿qué tan probable es que ocurra ese riesgo? Y ¿qué tan grande sería su impacto si sucede? Para ello, evaluamos el Nivel de Riesgo Inherente (es decir, antes de mitigarlo) y el

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	Viñetas digitales que indiquen riesgo. Controlar Animación de una barrera protectora. Monitorear Diferentes monitores alrededor.	Nivel de Riesgo Residual (esto es, después de mitigarlo). Y los clasificamos en niveles que van desde los más críticos hasta los más bajos. • Luego pasamos al control, donde establecemos medidas para mitigar esos riesgos, reduciendo su probabilidad e impacto. • Finalmente, monitoreamos, o sea, realizamos un seguimiento continuo para asegurar que los controles funcionen correctamente. Y si algo no va bien, ¡lo corregimos!
Música dinámica y jovial de fondo.	[Textos en pantalla:] Tratamiento de riesgos Evitar o eliminar el riesgo Un escudo. Mitigar el riesgo Diferentes candados. Transferir el riesgo Animación de una póliza de seguros. Aceptar el riesgo Símbolo de palomita (check mark).	¿Y cómo tratamos con los riesgos? ¡Tenemos varios caminos! • Una opción es evitar o eliminar el riesgo, es decir, abstenerse de realizar la actividad que podría generarlo. Por ejemplo, si un proyecto es demasiado arriesgado, optamos por no llevarlo a cabo. • Otra posibilidad es mitigar el riesgo, aplicando medidas para disminuir la posibilidad de que ocurra; puede ser a través de nuevos controles o mejoras en los procesos. • Otra opción es transferir el riesgo. Por ejemplo, contratando un seguro para que un tercero se haga cargo de las posibles pérdidas. • También es posible aceptar el riesgo, si consideramos que el costo de mitigarlo es mayor que su posible impacto.
	[Texto en pantalla:] ¿Se puede no gestionar los riesgos?	¡Ahora hablemos de algo muy importante!: ¿qué pasa si no gestionamos los riesgos? Pues podríamos enfrentar demandas legales, multas, pérdidas económicas, fraudes, reprocesos y

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	¡La respuesta es NO! Ícono de advertencia.	sobrecostos en las operaciones e, incluso, ¡perder la confianza de nuestros clientes! Un panorama bastante negativo, ¿no crees?
Música dinámica y jovial de fondo.	[Texto en pantalla:] Plan de remediación	Por último, cuando algo sale mal, en SURA Asset Management contamos con el Plan de Remediación , que nos ayuda a definir acciones, responsables y tiempos para enfrentar el riesgo de la mejor manera posible.
Cambio de música para dar paso a conclusiones.	[Textos en pantalla que se van “palomeando” como checklist:] Tipos de riesgo Riesgos operacionales Etapas de gestión de riesgos Tratamiento de riesgos Planes de remediación	Hagamos un breve recuento de lo que vimos sobre este tema: • Hay varios tipos de riesgo: operacionales, legales, reputacionales, financieros y estratégicos. • Los riesgos operacionales incluyen: fraudes internos y externos, incumplimiento de la legislación laboral, daños a activos físicos, fallas tecnológicas, errores en los procesos, así como malas prácticas que afectan a los clientes. • Los riesgos se gestionan a través de diferentes etapas: identificación, medición, control y monitoreo. • Ante un riesgo, es posible: evitarlo, mitigarlo, transferirlo a un tercero, o aceptarlo si así conviene al negocio. • Los planes de remediación definen acciones para enfrentar un riesgo.
Música de cierre.	Conductor concluye este tema.	¡Muchas gracias por acompañarme en este tema tan interesante! Ahora pasemos al siguiente punto: ¡la Ley Sarbanes-Oxley!
Sonido de cortinilla.	[Cortinilla:] Ley Sarbanes-Oxley Conductor a cuadro.	(SOX) Conductor:

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	[Texto en pantalla:] Ley Sarbanes-Oxley Imagen digital de una balanza que represente justicia. Imágenes de titulares de escándalos financieros. Signos de pesos. Candado virtual. Van apareciendo íconos de:	¡Ya estamos de regreso! Ahora abordaremos un tema que no solo tiene que ver con reglas financieras, sino también con la transparencia y la ética de las empresas: la Ley Sarbanes-Oxley, también conocida como SOX. Esta ley surgió en el 2002, en Estados Unidos, después de los mega escándalos de Enron y WorldCom, compañías que cometieron fraudes gigantescos y afectaron la confianza en los informes financieros. Para que esto no volviera a pasar nació la Ley SOX, que busca garantizar la transparencia y la integridad de los informes financieros... ¡y claro, evitar fraudes! La Ley SOX exige que las empresas implementen controles internos sólidos. Aquí te cuento algunos puntos clave que debes saber sobre ella:
Música dinámica y jovial de fondo.	Un edificio con un signo de aprobación. Martillo de un juez. Ejecutivos.	• Estableció un organismo para supervisar los estados financieros de las compañías. • Reforzó las sanciones contra el fraude corporativo. • E impuso requisitos para la Alta Dirección de las compañías y para que un auditor independiente evalúe la efectividad del control interno.
	[Van apareciendo esferas con los puntos clave y se unen en una misma para que aparezca en el centro la palabra: Transparencia] Consolidamos buenas prácticas. Fortalecemos nuestra cultura ética. Prevenimos fraudes y mala gestión.	Para SURA AM, cumplir con lo que establece la Ley SOX es muy importante, ¡porque nos ayuda a ser éticos, responsables y transparentes! Gracias a ella: • Consolidamos buenas prácticas contables y financieras. • Fortalecemos una cultura de responsabilidad y ética sobre la precisión de los informes financieros. • Y prevenimos fraudes y una mala gestión financiera.

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	TRANSPARENCIA	
Música dinámica y jovial de fondo.	[Texto en pantalla:] Marco COSO Aparece esquema del Marco COSO (página 9 del documento). Los cinco componentes se muestran como bloques flotantes alrededor del conductor: Evaluación del riesgo Ambiente de control Información y comunicación Actividades de control Monitoreo Se muestran los cinco bloques del Marco COSO conectados entres sí con líneas que brillan al unirse.	Para cumplir con esta ley, contamos con nuestro Sistema de Control Interno (o SCI), que se basa en el Marco COSO, siglas en inglés del Comité de Organizaciones Patrocinadoras de la Comisión Treadway, una organización internacional líder en la gestión de riesgos. El Marco COSO establece cinco componentes para que nuestro Sistema de Control Interno sea efectivo, evitando deficiencias que afecten nuestra información financiera: 1. Evaluación del riesgo. 2. Ambiente de control. 3. Información y comunicación. 4. Actividades de control. 5. Y monitoreo. Para lograr la mayor efectividad, es fundamental que los cinco componentes operen de forma conjunta e integrada.
Música dinámica y jovial de fondo.	Aparece un gráfico con dos círculos, uno con el texto "Evaluación interna" y otro con "Auditoría externa". Un documento siendo firmado.	¡Y siempre estamos revisando cómo van las cosas para mejorarlas! Por ello se realizan evaluaciones tanto internas como externas para asegurar que el Sistema de Control Interno funcione correctamente. Tanto las autoevaluaciones como las auditorías independientes nos ayudan a identificar cualquier brecha o área de mejora en nuestros controles. Los resultados de esas evaluaciones son firmados por los líderes de los subprocesos, los responsables de los estados financieros y los líderes de la compañía.

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	Ejecutivos trabajando. [Textos en pantalla:] Cumplir con políticas y controles. Reportar irregularidades. Formación constante. Mesa de directores. Ejecutivos dándose la mano.	¡Y ojo! ¡Cada uno de nosotros tenemos un rol esencial en todo esto! Para contribuir a que nuestro Sistema de Control Interno funcione adecuadamente, todos en la compañía debemos: • Cumplir con los principios, políticas, procedimientos y controles internos. • Reportar toda irregularidad que pudiera afectar la integridad de los informes financieros. • Y recibir formación sobre la Ley SOX y las políticas de la compañía relacionadas con el control interno. Por su parte, la Junta Directiva tiene el deber de guiar, asesorar y vigilar la correcta implementación y eficacia del Sistema de Control Interno. Cumplir con la Ley SOX no solo es una obligación, ¡es una responsabilidad ética! Y eso nos permite mantener la confianza de los inversionistas y los diferentes grupos de interés.
Cambio de música para dar paso a conclusiones. Música de cierre de segmento.	[Textos en pantalla:] Transparencia e integridad Información financiera impecable Todos contribuimos Conductor se despide sonriente.	Así que, para resumir, aquí aprendimos que: • La Ley SOX establece estrictas reglas para garantizar la transparencia y la integridad de los informes financieros. • El Marco COSO especifica los componentes necesarios para que los controles funcionen correctamente y nuestra información financiera sea impecable. • Todos en SURA Asset Management cumplimos un rol fundamental para garantizar que la información financiera de sea íntegra y transparente. ¡Juntos cuidamos a nuestra compañía! ¡Nos vemos en el siguiente segmento!

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Sonido de cortinilla. Música dinámica de inicio de segmento.	[Cortinilla:] Seguridad de la información y ciberseguridad Conductor a cuadro, sonriente. Un candado gigante que se cierra. 	[Segmento 3. Seguridad de la información y ciberseguridad] ¡Hola! Bienvenidos a un nuevo segmento. Aquí hablaremos de la seguridad de la información y la ciberseguridad. Hoy más que nunca, la información es uno de los activos más valiosos para cualquier organización, ¡y en SURA Asset Management lo sabemos muy bien! Pero ¿por qué es tan importante proteger la información? ¡Ahora te digo!
Música dinámica y jovial de fondo.	[Textos en pantalla:] Seguridad de la información Confidencialidad Integridad Disponibilidad Gráficos que representen datos, intercambio de información. Aparece un gran sello de "confianza" que se plasma a un lado del logo de SURA AM. [Texto en pantalla:] Información confidencial Carpeta con sello de "top secret". Un jenga que se viene abajo.	Primero comencemos diciendo qué es la seguridad de la información. Son las medidas que implementamos para proteger la confidencialidad, integridad y disponibilidad de la información. Esto implica que solo las personas autorizadas accedan a determinados datos, que la información no pueda ser alterada sin permiso y que esté disponible cuando sea necesario. Esta es la base de la confianza digital, algo fundamental en el mundo de los negocios ¡y por supuesto, en nuestra compañía! En nuestra actividad profesional, cada uno de nosotros manejamos diferentes tipos de información, y es importante identificarlos para saber qué clase de protección necesita cada uno. Por ejemplo, la información confidencial, que es clave para el negocio, solo puede ser gestionada por personal autorizado, y requiere de permisos y medidas de protección adicionales para ser compartida con personas externas. Si nuestra información confidencial llegara a las manos equivocadas, ¡podríamos enfrentar

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	[Texto en pantalla:] Información pública Gráficos que reflejen envío de información. Ícono de mail. Logo de Gmail tachado. Ícono de papelera vacía. Ícono de carpeta compartida. Ícono de mensaje que se envía.	consecuencias muy serias! Por ejemplo: daños a nuestra reputación, pérdidas económicas e incluso sanciones por incumplir la legislación sobre protección de datos. Así que si tú manejas información confidencial, ¡sé muy cuidadoso! En cambio, la información pública no tiene restricciones y puede compartirse sin problema. Toda información tiene un propietario interno, que no necesariamente es tu líder o dueño del proceso; por ejemplo: la información del cliente le pertenece a él, mientras que la de nómina corresponde a una persona de Talento Humano. Así que cuando necesites compartir información confidencial, solo podrás hacerlo si cuentas con la autorización de su propietario, tomando estas medidas: • Usa únicamente los medios de la compañía. ¡Nada de utilizar correos personales ni almacenar la información en plataformas públicas como Gmail, Hotmail o Yahoo! • Elimina la información cuando ya no la uses, ya sea digital o física. ¡No guardes archivos de manera innecesaria y destruye los papeles! • Comparte carpetas solo con personas autorizadas ¡y no le des acceso a “todos los usuarios”! • Si necesitas compartir información con terceros, hazlo únicamente a través de medios corporativos, comprueba si están autorizados y verifica que se cumplan las cláusulas de confidencialidad.
	[Texto en pantalla:] Consejos de seguridad en internet Gráficos o íconos de actividad en línea: Ícono de cursor.	Ahora te voy a dar algunos consejos de seguridad para usar internet que no solo te servirán para el trabajo, ¡sino también para tu vida personal! • Utiliza una conexión de internet segura. • Crea contraseñas difíciles de replicar.

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	Ícono de password. Huella digital Computadora. Sitio web. Ícono de red social. Un anuncio en línea Ícono de engrane de "configuración". Íconos de archivos. Candado. Ícono de chat en línea. Ícono de antivirus	• Habilita la autenticación multifactorial siempre que sea posible. • Mantén el software y el sistema operativo actualizados. • Comprueba que los sitios web que visitas sean confiables. • Revisa la configuración y las políticas de privacidad. • Ten mucho cuidado con los vínculos sospechosos. • Comprueba que tus dispositivos estén protegidos. • Haz copias de seguridad de manera periódica. • Cierra las cuentas que no utilices. • Sé cuidadoso con lo que descargas, lo que publicas y con quién interactúas en internet. • Utiliza un antivirus confiable y mantenlo actualizado.
Música dinámica y jovial de fondo.	[Texto en pantalla:] Incidentes de seguridad Accidentales Un archivo que está siendo borrado. Intencionales Ícono de robo. Causados por ciberdelincuentes Ícono de ciberpirata.	Hablemos ahora de los incidentes de seguridad. ¿Sabías que hay tres tipos? ¡Aquí te los explico! 1. Accidentales. Ocurren cuando cometemos errores sin querer. ¿Quién no ha borrado un archivo por accidente o ha enviado un correo a la persona equivocada? Incluso podemos dañar un disco duro de manera involuntaria. 2. Intencionales. Son los realizados por colaboradores (o insiders). ¡Aquí las cosas se ponen serias! Es cuando un colaborador, por enojo o por influencia externa, decide robar información o dar acceso a alguien que no debería tenerlo. 3. Causados por ciberdelincuentes. Los ciberdelincuentes son especialistas en encontrar fallas en los sistemas o engañarnos para robar información a través de software malicioso o malware. Algunos ejemplos son:

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	[Texto en pantalla:] Ejemplos de malware	○ Los troyanos, es decir, software que roba información. ○ El ransomware, software que bloquea acceso a la información y exige un rescate. ○ O los botnets, software que convierte nuestros dispositivos en herramientas para actividades delictivas.
	Ícono de malware.	Aquí lo importante es saber que el malware puede infectar tus dispositivos mediante archivos adjuntos, enlaces a sitios web, links en anuncios fraudulentos o aprovechando alguna vulnerabilidad de los navegadores. Una vez en tu equipo, podría distribuirse a través de la red corporativa. ¡Así que ten mucho cuidado!
	El conductor señala un letrero de alerta al lado de una imagen de un ciberdelincuente.	¡Es sorprendente cómo los ciberdelincuentes pueden atacarnos ante el menor descuido! Por ello siempre debemos estar alertas y ser muy cautelosos con lo que hagamos en línea.
Música dinámica y jovial de fondo.	Imagen de sistemas de cómputo.	Es momento de hablar de la ciberseguridad . Se trata de las medidas destinadas a proteger la información y a gestionar las amenazas tanto de los sistemas conectados entre sí, como de los conectados al ciberespacio.
	[Texto en pantalla:] Tips de ciberseguridad	Aquí te van algunos tips de ciberseguridad al usar el correo electrónico, al estar en tu puesto de trabajo o al utilizar las redes sociales.
	Íconos de correo electrónico.	Comencemos con el correo electrónico , esa herramienta tan útil, ¡pero también tan peligrosa! Todos lo usamos a diario y desafortunadamente es el punto de entrada favorito de los ciberdelincuentes.
	Letrero de spam.	Es muy común recibir en nuestro buzón corporativo correos no deseados o spam, o mensajes que fingen ser de personas u organizaciones conocidas.
	[Texto en pantalla:] Tipos de fraudes por correo	Hay varios tipos fraudes por correo que debemos reconocer:

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	Gráficos de phishing. Notificación de correo recibido. [Texto en pantalla:] Scam Mail con el asunto de “¡Ganaste un premio!” [Texto en pantalla:] Sextorsión Ícono de criptomonedas. [Texto en pantalla:] Tips para detectar correos fraudulentos. [En texto (palomeado):] contacto@banco.com [En texto (tachado):] contacto@juanperez.com	1. El phishing, que busca engañar a la gente haciéndose pasar por una entidad confiable, como un banco, una red social o entidades públicas como la autoridad tributaria, con el objetivo de robar contraseñas o datos personales. Generalmente se intentan cometer estos fraudes a través del correo, pero también con mensajes SMS, de WhatsApp o de otras aplicaciones. 2. Scam: Este tipo de fraude promete cosas como premios, herencias millonarias u ofertas de empleo, pero lo único que busca es engañarte y robarte dinero o información personal o de tu empresa. 3. Sextorsión. Aquí amenazan con difundir videos privados o de contenido comprometedor si el usuario no paga una suma de dinero. El pago generalmente es solicitado en criptomonedas como el bitcoin. Recuerda: todos estos mensajes son solo un truco, ¡no caigas! Si ves un correo raro o sospechoso, ¡detente y revísalo con cuidado! Aquí te comparto algunos tips para detectar correos fraudulentos: • Revisa el remitente: Los ciberdelincuentes suelen utilizar direcciones de correo falsas. Por ejemplo, en los correos bancarios legítimos, normalmente se emplea el nombre de la institución después de la arroba. Pero cuando una dirección es falsa, tiene nombres que no tienen nada que ver. Por eso es importante observar el remitente a detalle, porque el cambio en una simple letra puede ser una señal de que algo no anda bien. También, si sospechas que se trata de una dirección ilegítima, puedes utilizar herramientas como Messageheader, de Google, para revisarla.
---	---	---

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	Imagen de una firma de correo de alguien de SURA AM. Un reloj que está corriendo rápidamente. [Mensaje de mail que inicia con:] Estimado cliente: Le informamos...	• Presta atención a la firma: Si el correo no tiene una firma oficial, o si parece distinta a la habitual, ¡desconfía! • Ten cuidado si el mensaje es “urgente”: Si te piden actuar rápidamente, ¡detente! Los ciberdelincuentes intentan que tomes decisiones sin pensar. Utilizan correos que parecen legítimos para presionarte a que abras un archivo malicioso, ingreses a una página web falsa o realices un pago. • Desconfía de los mensajes impersonales: Los correos fraudulentos comúnmente se refieren al destinatario de manera muy general, como “usuario” o “cliente”, mientras que las organizaciones legítimas usan el nombre y los apellidos.
Música dinámica y jovial de fondo.	Íconos de attachment files. Aparecen íconos de archivos con estas terminaciones y el conductor los señala: .exe .vbs .docm .xlsm .pptm Íconos de carpetas comprimidas Una lupa revisando un mail.	• Sé precavido con los documentos adjuntos o enlaces: ¡Nunca abras un archivo si no estás seguro de quién lo envió! Ten en cuenta que los bancos o las instituciones públicas no envían archivos a través de correos. En todo caso, estos se descargan directamente desde el portal o la aplicación oficial de la entidad. Recuerda que los archivos adjuntos pueden ser usados para distribuir malware. Por eso, ¡mucho ojo con los documentos que tienen estas extensiones, ya que son muy peligrosos! (el conductor señala los íconos con las extensiones de archivos peligrosos) También las carpetas comprimidas .zip o .rar son potencialmente peligrosas; solo deberías abrirlas si el remitente es cien por ciento confiable. • Desconfía si el correo está mal escrito. Las faltas de ortografía o una redacción

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

		deficiente también son señales de un posible fraude. ¡Recuerda! Si alguna vez tienes dudas, verifica directamente con la persona o entidad que supuestamente te contactó.
Música dinámica y jovial de fondo.	[Texto en pantalla:] Seguridad en el puesto de trabajo Un escritorio limpio. Una laptop cerrada. Escoleo en una red social.	Hablemos ahora de la seguridad en el puesto de trabajo. Aquí también debemos tomar medidas para proteger la información: 1. Deja la mesa despejada. Al final de tu jornada, guarda toda la documentación visible, especialmente en espacios compartidos o públicos. ¡Evita que cualquier persona acceda a tu información! 2. Bloquea la sesión. Si te alejas de tu computadora, ¡bloquéala! Así protegerás tus documentos y evitarás que alguien acceda a tu información sin permiso. 3. Usa adecuadamente internet y los sistemas corporativos. Solo utiliza los recursos de la empresa para trabajo. Evita navegar en sitios inseguros o hacer actividades personales que pongan en riesgo los sistemas.
Música dinámica y jovial de fondo.	[Texto en pantalla:] Medidas de seguridad en redes sociales Gráficos que representen redes sociales. [Textos en pantalla:] Contraseñas fuertes Aparece un ícono de password. Autenticación en dos pasos Ícono de huella digital	Existen medidas adicionales que pueden ayudar a mejorar la seguridad de nuestra información al usar aplicaciones o redes sociales: • Contraseñas fuertes: Usa claves largas y complejas. ¡Evita las obvias! Y cámbialas de vez en cuando. • Autenticación en dos pasos: Activa el doble factor de autenticación en todos tus accesos importantes. ¡Es como una cerradura extra! Consiste en añadir otro

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	Sentido común Celular con viñetas de reacciones de redes Emoji de enojo Íconos que indiquen malas palabras: \$%&\$@! Botón de “reenviar” tachado. Gráfico de “confidencial” [Texto en pantalla:] Configuración de privacidad. Cuidado con los adjuntos y los enlaces. No registrarse con el correo corporativo.	paso, como una huella digital o un código especial, para poder acceder. • Sentido común: Antes de publicar algo en las redes sociales, piensa si puede dañar la imagen de la empresa. ¡Tu comportamiento en línea también afecta la seguridad! Así que evita: ○ Emitir comentarios negativos, como quejas laborales. ○ Enfrascarte con otros usuarios en discusiones sin sentido, así como insultar, amenazar o acosar. ○ Propagar noticias sin confirmar si son verdaderas o falsas. ○ Compartir información confidencial o sujeta a propiedad intelectual. • Configuración de privacidad: Asegúrate de configurar correctamente las opciones de privacidad en tus perfiles de redes sociales. ¡Limita quién puede ver lo que publicas! • No descargues documentos adjuntos sin antes escanearlos con un antivirus o con herramientas como VirusTotal, y nunca des clic a enlaces sospechosos. • No utilices el correo corporativo para registrarte en alguna red social, <i>app</i> o cualquier otra plataforma externa a la organización.
Música dinámica y jovial de fondo.	[Texto en pantalla:] Área de Seguridad de la Información Imágenes de especialistas de TI.	Recuerda que el área de Seguridad de la Información es nuestro mejor aliado para evitar o atender incidentes de seguridad. Así que si detectas situaciones sospechosas como las siguientes, ¡repórtalas!: • Como cuando alguien envía una base de datos con información confidencial sin estar autorizado. • Cuando una persona instala software no permitido en las computadoras.

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	Imágenes oscuras o en blanco y negro de personas utilizando computadoras, dando a entender que están realizando actividades deshonestas. Ícono de ciberataque. Manos de una persona entregando un folder a otra.	• Cuando alguien utiliza usuarios y contraseñas de otras personas. • Cuando alguien intenta acceder a los sistemas para realizar actividades que no le corresponden. • Cuando una persona intenta acceder a servicios en internet para compartir información sin estar autorizada. • Cuando tú o algún compañero sospecha que ha sido víctima de un ciberdelito, incidente de seguridad o robo de identidad digital. • O cuando una persona toma documentos físicos de los puestos de trabajo sin autorización.
Cambio de música para dar paso a conclusiones.	[Textos en pantalla en forma de checklist:] Proteger la información Solo personal autorizado Seguridad en internet El peligro del malware Evitar caer en fraudes Recurrir al área de Seguridad de la Información	Recapitulando, en este segmento aprendimos que: • El término seguridad de la información se refiere a las medidas para proteger la confidencialidad, la integridad y la disponibilidad de los datos. • La información confidencial solo puede ser manejada por personal autorizado tomando diferentes medidas para protegerla. • Debemos cuidar que nuestra actividad en internet sea segura. • Si no somos cuidadosos, algún tipo de malware puede infectar nuestros dispositivos y distribuirse por la red corporativa. • Tenemos que seguir las recomendaciones para no caer en fraudes como el phishing, el scam o la sextorsión. • Debemos recurrir al área de Seguridad de la Información ante cualquier incidente de seguridad o situación sospechosa.
Música inspiradora de cierre.	Conductor se despide	¡Y recuerda! La seguridad de la información y la ciberseguridad es responsabilidad de todos. Si seguimos las recomendaciones, ¡estaremos mucho más protegidos! ¡Gracias por acompañarme! ¡Nos vemos en el próximo segmento!

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Sonido de cortinilla. Música dinámica de inicio de segmento. Música dinámica y jovial de fondo.	[Cortinilla:] Gestión de la Continuidad del Negocio Pólizas Desaparece “Pólizas” para indicar que comenzaremos con “Gestión de la Continuidad del Negocio” Conductor a cuadro. Imágenes de gente trabajando en oficinas.	[Segmento 4. Gestión de la Continuidad del Negocio y Pólizas] (Gestión de la Continuidad del Negocio) ¡Hola! Bienvenido a otro segmento súper interesante. Comenzaremos hablando de la Gestión de la Continuidad de Negocio. Suena a algo muy técnico, pero te lo voy a explicar de manera sencilla. Empecemos definiendo qué es. Bueno, básicamente es una estrategia para que las operaciones no se frenen cuando ocurren situaciones excepcionales. La idea es que, si algo interrumpe nuestras operaciones, podamos reaccionar rápido y minimizar el impacto, para volver a la normalidad lo más rápido posible y atender como se debe a los grupos de interés.
Música dinámica y jovial de fondo.	[Texto en pantalla:] Tipos de amenazas [Texto en pantalla:] Amenazas naturales Gráficos de terremotos, incendios, tormentas, pandemia. [Texto en pantalla:] Amenazas provocadas por personas Explosiones. Hacker en acción.	¿Pero qué amenazas podrían interrumpir nuestras operaciones? Te menciono algunas: Están las amenazas naturales, que se dividen en diferentes tipos: • Geológicas, como los terremotos. • Meteorológicas, como inundaciones, incendios, tormentas, descargas eléctricas y contaminación. • Y biológicas, como las enfermedades y pandemias. También hay amenazas provocadas por el ser humano. Entre ellas están: • Las accidentales, como la interrupción o pérdida de energía eléctrica, daños en la infraestructura o explosiones. • Y las intencionales, como actos de terrorismo, sabotajes, huelgas, pérdida o

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	[Texto en pantalla:] Amenazas tecnológicas Mensaje de error en una computadora. Varias computadoras. Computadora hackeada. [Listado con el símbolo de advertencia (!):] Acceso al sitio de trabajo Personal clave Proveedores Acceso a aplicaciones Íconos de envíos de mensajes.	robo de la información, o daños causados por colaboradores insatisfechos. Y no olvidemos las amenazas tecnológicas, como: • Fallas de los servicios de computación y de las telecomunicaciones. • Cambios tecnológicos que afecten el servicio. • Sabotaje informático, como los ciberataques, el robo de identidad, acceso no autorizado, secuestro de la información, código malicioso, fraudes y todo lo que revisamos en el segmento de <i>Seguridad de la información y ciberseguridad</i>. Como pueden ver, las amenazas son muy variadas, pero todas tienen un común denominador: ¡pueden interrumpir nuestras operaciones! ¿Y qué situaciones se pueden generar a causa de ellas? • No poder acceder al sitio de trabajo, lo que alteraría la operación normal de la compañía. • Falta de personal clave para realizar las actividades. • Ausencia de proveedores críticos. • Y falta de acceso a las aplicaciones o información esencial. ¡Y aquí es donde entra el Plan de Comunicaciones!, diseñado para informar qué deben hacer los colaboradores durante y después del incidente. ¡Es muy importante que todos estemos súper atentos a la información que se emite!
	[Texto en pantalla:] Acciones ante un incidente	¿Qué debemos hacer cuando ocurre un incidente?

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	El conductor señala un diagrama de flujo, que representa la cadena de mando ante una crisis. [Texto en pantalla:] Comité de crisis Piezas de ajedrez que se mueven a gran velocidad. [Textos en pantalla:] Aprobar marco de actuación.	- Lo primero es reportarlo al líder de Continuidad del Negocio, quien se encargará de analizar el problema y coordinar la reacción junto con los responsables de la contención, la respuesta y la recuperación frente al incidente. También liderará la activación de los planes contingentes en caso de que se superen los tiempos para que las operaciones vuelvan a la normalidad. - Si el problema es muy grave y representa un serio impacto a nivel reputacional, financiero o legal, el Comité de Crisis entrará en acción, tomando decisiones clave, como si moviera las piezas de un ajedrez: Aprobar el marco de actuación para eventos de gran magnitud que afecten la integridad de los colaboradores, las instalaciones y la información confidencial. Asignar los recursos necesarios y agilizar los trámites para solucionar el problema de manera eficiente. Aprobar o rechazar las solicitudes del equipo que ejecuta el Plan de Continuidad con respecto a temas legales, relaciones institucionales, seguros, responsabilidad civil ante daños a terceros, entre otros. Comunicar a los interesados el estatus de la situación. Y definir el momento adecuado para retomar la operación normal.
Música dinámica y jovial de fondo.	Asignar recursos Aprobar solicitudes Comunicar Retornar a la normalidad	
Música dinámica y jovial de fondo.	Se despliega un diagrama con varios círculos interconectados. En el centro irá el ícono de un ejecutivo y alrededor las responsabilidades: Implementar controles Definir estrategias	Si tú trabajas en un subproceso crítico para la continuidad del negocio, tienes varias responsabilidades muy importantes, como: Diseñar e implementar controles para mitigar los riesgos. Definir estrategias y generar, actualizar y optimizar continuamente los procedimientos

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	Participar en pruebas Capacitarse	de recuperación para que la operación vuelva a la normalidad. • Participar en las pruebas de continuidad de negocio para verificar los planes de recuperación. • Capacitarte constantemente en tu subproceso y capacitar a otros colaboradores que pueda apoyar en caso de que estés ausente.
Música dinámica y jovial de fondo.	[Textos en pantalla:] Estrategias de recuperación 1. Prevención 2. Mitigación 3. Recuperación	Las estrategias de recuperación se enfocan en tres puntos clave: 1. Prevención: Evitar que los incidentes ocurran. 2. Mitigación: Hacer todo lo posible para reducir el impacto si algo sucede. 3. Recuperación: Regresar a la normalidad lo antes posible.
Música dinámica y jovial de fondo.	Gráficas digitales de maquinarias y procesos que funcionan perfectamente.	Pero no basta con tener todo planeado, ¡también hay que comprobar que funcione! Para ello, nuestra empresa realiza pruebas del Plan de Continuidad de Negocio y del Plan de Recuperación de Desastres de Tecnología , que permiten: • Detectar posibles fallas y realizar ajustes. • Garantizar que los equipos estén conformados y listos para reaccionar. • Validar que los planes estén documentados y actualizados. • Comprobar que los colaboradores conocen a la perfección lo que deben hacer para activar los planes. • Y verificar que se cuenta con los recursos necesarios.
	Flechas dirigiéndose a una misma dirección.	¡Y ahí lo tienes! Ahora ya sabes que la Gestión de la Continuidad del Negocio implica tener planes para reaccionar de manera eficiente y

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Cambio a música motivadora de cierre.	Conductor se despide con una sonrisa.	eficaz ante cualquier emergencia, a fin de regresar a la normalidad lo antes posible. Si alguna vez enfrentamos un desafío que ponga en riesgo nuestras operaciones, hay una estrategia detrás para recuperar el control. ¡Y todos debemos estar listos para saber cómo reaccionar! ¡Pasemos al siguiente tema de este segmento!
Sonido de cortinilla. Música dinámica de inicio de tema. Música dinámica y jovial de fondo.	[Cortinilla de:] Pólizas Conductor a cuadro. Ícono de póliza de seguros. [Texto en pantalla:] Seguro de daños Íconos de casas y coches. [Texto en pantalla:] Seguro de personas Ícono de una familia.	(Pólizas) Conductor: Ahora hablaremos de las pólizas de seguro. Empecemos definiendo qué son los seguros: son como una especie de “red de seguridad financiera”, es decir, instrumentos que minimizan el impacto económico cuando pasa algo inesperado. Se clasifican en dos grupos: - El primer grupo son los seguros de daños, que incluyen: - Los seguros de propiedad, los cuales cubren bienes muebles o inmuebles. - Y los seguros patrimoniales, que amparan el patrimonio de las personas, por ejemplo, cuando deben asumir una responsabilidad frente a otros en caso de un accidente. - El segundo grupo son los seguros de personas, que amparan la vida, la integridad y la salud de los individuos.
	[Van apareciendo los textos de:] Partes del contrato Vigencia Suma asegurada Prima	¿Y qué debe incluir una póliza de seguro? Debe especificar esta información: - Las partes del contrato. - La vigencia. - La suma asegurada y cómo se calcula. - El precio del seguro o la prima.

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

Música dinámica y jovial de fondo.	Riesgos que cubre [Aparecen las palabras de:] Futuro Incierto Medible [Textos en pantalla:] Condiciones del producto Coberturas Condiciones Ícono de manos estrechándose.	Así como los riesgos que cubre y los que quedan excluidos. Y ojo, no todos los riesgos pueden cubrirse. Para que un riesgo pueda ser asegurado, debe ser futuro, incierto y medible. Es decir, no puede tratarse de situaciones que ya hayan pasado ni que sean totalmente predecibles. ¿Y qué es lo que debe saber el asegurado? Es fundamental que conozca las condiciones del producto, las coberturas que ofrece y los posibles cambios en las condiciones de su póliza. También es muy importante que el asegurado declare el estado real del riesgo, porque si omite información o proporciona datos inexactos, puede ocasionar que se invalide su contrato.
Música dinámica y jovial de fondo.	Aparece un gráfico flotando que representa a Latinoamérica en su conjunto y otro que resalta a los diferentes países. [Donde se queda flotando el mapa que representa a toda la región aparecen los textos:] Programa regional Seguro Global Bancario Seguro para Asesores e Instituciones Financieras Seguro para Miembros de la Junta y Administradores Seguro contra ciberataques	Hablemos ahora del programa de pólizas para SURA Asset Management, que se divide en dos: el programa regional y el programa de pólizas locales. El programa regional incluye las pólizas de líneas financieras, como: El Seguro Global Bancario, que protege contra fraudes realizados por colaboradores de la compañía. El Seguro de Responsabilidad Civil Profesional para Asesores de Inversión y para Instituciones Financieras, que protege a las compañías frente a los riesgos relacionados con su actividad. El de Responsabilidad para Miembros de la Junta y demás Administradores, que otorga cobertura a los integrantes de Juntas Directivas y Administradores. - Y finalmente, está el Seguro Cyber, que brinda protección contra ciberataques y riesgos informáticos.

GUION VIDEO CURSO ANUAL DE RIESGOS SURA AM

	[Donde se queda flotando el mapa que representa a los países aparecen los textos:] Programa local Seguros para personas Pólizas de vida	El programa local, por su parte, contempla otras pólizas necesarias para operar de acuerdo con el apetito de riesgo. Esto incluye los seguros de personas, como las pólizas de vida que cada empresa contrata según las políticas locales.
Cambio de música para conclusiones	[Aparecen en forma de checklist los textos:] Los seguros minimizan el impacto económico Se clasifican en seguros de daños y seguros de personas Nuestro programa de pólizas se divide en: programa regional y programa local	En resumen, sobre el tema de pólizas revisamos que: • Los seguros son instrumentos financieros que minimizan el impacto económico cuando ocurre un suceso inesperado. • Los seguros se clasifican en dos grupos: de daños (que incluyen los seguros de propiedad y los patrimoniales) y de personas (que amparan la vida, la integridad y la salud). • SURA Asset Management cuenta con un programa de pólizas que se divide en dos: un programa regional y programa de pólizas locales.
Música de cierre.	Conductor se despide con una sonrisa.	Con este segmento concluimos el Curso de Riesgos de SURA Asset Management. Gracias por tu interés y te recordamos que, para proteger a nuestra empresa de los riesgos, tú eres un gran aliado. ¡Hasta la próxima!