

<b>Control de Acceso</b>	
Cantidad de objetivos de control	7
Cantidad de controles	25
Total de preguntas	50

<b>11.1</b>
<b>Objetivo</b>

<b>11.1.1</b>
---------------

<b>Requerimientos del negocio para el control de acceso</b>	
Controlar el acceso a la información	

<b>Política de control de acceso</b>	
--------------------------------------	--

Esta definida y documentada la política de control de acceso que contemple las necesidades del negocio y además requerimientos de seguridad para el acceso a los diferentes recursos

	<input type="radio"/> SI <input checked="" type="radio"/> NO
--	--

En la política de acceso definida están claramente identificados los derechos de acceso tanto de usuarios como de grupos de usuarios

	<input type="radio"/> SI <input checked="" type="radio"/> NO, definida por el propietario <input type="radio"/> NO
--	--

Cual de los siguientes elementos no los contempla la política de control de acceso

	<input type="checkbox"/> Requerimientos de seguridad individuales de las aplicaciones del negocio <input type="checkbox"/> Difusión de información <input type="checkbox"/> Requerimientos legales y contractuales <input type="checkbox"/> Relación con la política de clasificación de la información <input type="checkbox"/> Consideraciones de la red <input checked="" type="checkbox"/> Segregación de roles de acceso <input type="checkbox"/> Autorización de los requerimientos de acceso <input type="checkbox"/> Revisiones periódicas de controles de acceso <input checked="" type="checkbox"/> Eliminación de derechos de acceso
--	---

Existen perfiles de acceso estándar para categorías comunes de trabajo

	<input type="radio"/> SI <input checked="" type="radio"/> NO
--	--

<b>11.2</b>
<b>Objetivo</b>

<b>11.2.1</b>
---------------

<b>Administración de acceso de usuarios</b>	
Garantizar el acceso autorizado de los usuarios y prevenir el acceso no autorizado a los sistemas de información	

<b>Registro de usuarios</b>	
-----------------------------	--

Existe un sistema formal de registro/cancelación de un registro de acceso a los servicios de procesamiento de información

	<input type="radio"/> SI <input checked="" type="radio"/> NO
--	--

Cual de los siguientes tópicos no son incluidos en el procedimiento de registro de usuarios

	<input type="checkbox"/> Autorización del propietario <input type="checkbox"/> Nivel de acceso apropiado <input checked="" type="checkbox"/> Uso de identificadores únicos <input type="checkbox"/> Validación de identificadores redundantes <input type="checkbox"/> Registro formal de todos los usuarios que usan servicios
--	---

Se le da a los usuarios una declaración escrita de sus privilegios, y se requiere que sea firmada por ellos de tal manera que entienda cuales son las condiciones de su acceso

	<input checked="" type="radio"/> Escrita y Firmada <input type="radio"/> Solo Escrita <input type="radio"/> Ninguno de los dos
--	--

Son removidas inmediatamente las cuentas de los usuarios que dejan la organización o son cambian de cargo dentro de la misma

	<input checked="" type="radio"/> SI <input type="radio"/> Solo cuando se va <input type="radio"/> Ambas, pero no de inmediato <input type="radio"/> No
--	--

<b>11.2.2</b>
---------------

<b>Administración de privilegios</b>	
--------------------------------------	--

Están restringidos y controlados cualquier tipo de privilegio especial que permita sobrepasar los controles del sistema o de la aplicación

	<input type="radio"/> SI <input checked="" type="radio"/> NO
--	--

Están identificados y definidos los privilegios de acceso con los productos de sistemas. Ej. Sistema operativo, bases de datos, así como las categorías de personal que lo pueden utilizar

	<input type="radio"/> SI, para ambos <input checked="" type="radio"/> SI, solo los privilegios <input type="radio"/> Ninguno de los dos
--	---

Los privilegios de los usuarios están asignados basados en la "necesidad de conocer" o por el principio "evento por evento"

	<input checked="" type="radio"/> SI <input type="radio"/> Necesidad de conocer únicamente <input type="radio"/> Evento por evento únicamente <input type="radio"/> Ninguno de los dos
--	---

Existe un proceso de autorización para asignar privilegios y guardar los registros de todos los privilegios asignados

	<input checked="" type="radio"/> SI <input type="radio"/> Autorización únicamente <input type="radio"/> Localización únicamente <input type="radio"/> Ninguno de los dos
--	--

Existen desarrollos y programas los cuales eviten la necesidad de tener privilegios de administrador

	<input type="radio"/> SI <input checked="" type="radio"/> NO
--	--

<b>11.2.3</b>
---------------

<b>Administración de contraseñas de usuario</b>	
---	--

La asignación de contraseñas esta controlada de manera segura

	<input checked="" type="radio"/> SI <input type="radio"/> NO
--	--

11.2.4

11.3  
Objetivo

11.3.1

11.3.2

11.3.3

11.4  
Objetivo

11.4.1

Requieren los usuarios firmar una declaración en la cual entienden que la contraseña es confidencial	
	<input type="radio"/> SI <input checked="" type="radio"/> NO
Si el usuario es quien mantiene el password, cual de los siguientes no aplica al usar el password temporal o nuevo	
	<input checked="" type="checkbox"/> Ubicación in-house de aplicaciones críticas
	<input type="checkbox"/> Aprobación del dueño del negocio
	<input checked="" type="checkbox"/> Implicaciones en la continuidad del negocio
	<input type="checkbox"/> Estándares de seguridad y cumplimiento
	<input type="checkbox"/> Procedimientos de manejo de incidentes
Revisión de los derechos de acceso de los usuarios	
Son los derechos de acceso de los usuarios revisados periódicamente	
	<input type="radio"/> SI <input checked="" type="radio"/> NO
Cuanto son revisados las capacidades de acceso de los usuarios	
	<input type="radio"/> Cada seis meses <input type="radio"/> Con mayor frecuencia <input checked="" type="radio"/> Con menor frecuencia <input type="radio"/> Nunca
Cuanto se revisan las autorizaciones para derechos de acceso privilegiados	
	<input type="radio"/> Cada seis meses <input type="radio"/> Con mayor frecuencia <input checked="" type="radio"/> Con menor frecuencia <input type="radio"/> Nunca
Son registrados los cambios de control de acceso para cuentas privilegiadas	
	<input type="radio"/> SI <input checked="" type="radio"/> NO
Es la asignación de privilegios revisada con regularidad	
	<input type="radio"/> SI <input checked="" type="radio"/> NO
Responsabilidades de los usuarios	
Prevenir acceso no autorizado de los usuarios, así como evitar posible tanto de información como de las instalaciones	
Uso del password	
Son comunicadas a los usuarios las buenas prácticas de seguridad en relación al uso y selección de la contraseña	
	<input checked="" type="radio"/> SI <input type="radio"/> NO
Cual de los siguientes tópicos en relación al uso de la contraseña no son dados a los usuarios	
	<input type="checkbox"/> Password son confidenciales
	<input checked="" type="checkbox"/> No escribir los password
	<input type="checkbox"/> Longitud mínima de la contraseña
	<input type="checkbox"/> Cambios del password de manera regular
	<input type="checkbox"/> Password difíciles de adivinar
	<input type="checkbox"/> Cambio de password en su primer Log-on
	<input checked="" type="checkbox"/> Nunca compartir el password
	<input type="checkbox"/> No usar directorios de palabras
Equipos de usuarios desatendidos	
Se le informa al usuario acerca de la importancia de mantener protegido un sistema desatendido	
	<input checked="" type="radio"/> SI <input type="radio"/> NO
Cual de los siguientes tópicos en relación al uso del computador no son dados a los usuarios	
	<input type="checkbox"/> Finalización de la sesión
	<input type="checkbox"/> Apagar el sistema al terminar
	<input checked="" type="checkbox"/> Bloqueo de la sesión cuando no se usa
Políticas de escritorio y pantallas limpias	
Se le informa al usuario acerca de la importancia de mantener un escritorio limpio	
	<input checked="" type="radio"/> SI <input type="radio"/> NO
Cuales de los siguientes elementos no son tenidos en cuenta en el momento mantener un escritorio limpio	
	<input type="checkbox"/> Información sensible o critica del negocio
	<input type="checkbox"/> Máquinas de fax
	<input type="checkbox"/> Uso de fotocopadoras
	<input checked="" type="checkbox"/> Impresión de documentos clasificados
Control de acceso en redes	
Evitar el acceso no autorizado a los servicios de red	
Política de uso de los servicios de red	
Existen los controles de red apropiados	
	<input checked="" type="radio"/> SI <input type="radio"/> No <input type="radio"/> No sabe <input type="radio"/> No aplica
Pueden los usuarios utilizar solamente los servicios de red a los que están autorizados	
	<input checked="" type="radio"/> SI <input type="radio"/> NO
Existe una política referente al uso de la red y de los servicios de red	
	<input checked="" type="radio"/> SI <input type="radio"/> NO

11.4.2	<p><b>Autenticación de los usuario para conexiones externas</b></p> <p>Cuando sea aplicable, son autenticadas las conexiones de los usuarios remotos vía una red pública u otra red que no sea de la compañía</p> <p><input checked="" type="radio"/> SI <input type="radio"/> NO</p> <p>Cuando sea aplicable, son autenticadas las conexiones de sistemas de cómputos remotos</p> <p><input checked="" type="radio"/> SI <input type="radio"/> NO</p>
11.4.3	<p><b>Identificación de equipos en la red</b></p> <p>Se ha considerado la identificación automática de equipos como medida para fortalecer desde ubicaciones de red específicas</p> <p><input checked="" type="radio"/> SI <input type="radio"/> No <input type="radio"/> No aplicable</p>
11.4.4	<p><b>Protección de puertos de diagnostico y configuración remotas</b></p> <p>Es controlado de manera segura el acceso a los puertos de diagnostico y/o configuración remotos de los dispositivos de red</p> <p><input checked="" type="radio"/> SI <input type="radio"/> NO</p>
11.4.5	<p><b>Segregación de redes</b></p> <p>Existe definido un perímetro que restringe las capacidades de conexión de los usuarios. Ej. Un firewall</p> <p><input checked="" type="radio"/> SI <input type="radio"/> NO</p>
11.4.6	<p><b>Control de conexión de red</b></p> <p>Han sido considerados los controles para restringir las capacidades de conexión de los usuarios. Ej. A través de gateway que filtren el tráfico</p> <p><input checked="" type="radio"/> SI <input type="radio"/> NO <input type="radio"/> No aplicable</p>
11.4.7	<p><b>Control de enrutamiento en redes</b></p> <p>Se han considerado los controles de enrutamiento</p> <p><input checked="" type="radio"/> SI <input type="radio"/> NO</p>
11.5	<p><b>Control de acceso al sistema operativo</b></p> <p>Evitar el acceso no autorizado al sistema operacional</p>
Objetivo	
11.5.1	<p><b>Procedimientos de log-on seguros</b></p> <p>Existen los apropiados controles de acceso en los sistemas operacionales</p> <p><input type="radio"/> SI <input checked="" type="radio"/> NO</p> <p>Cual de los siguientes elementos no es incluido en el proceso de log-on</p> <p><input type="checkbox"/> Identificación no desplegada del sistema</p> <p><input type="checkbox"/> Alarmas sobre acceso únicamente por personal autorizado</p> <p><input type="checkbox"/> No mostrar mensajes de ayuda</p> <p><input type="checkbox"/> Limite de intentos de log-on</p> <p><input checked="" type="checkbox"/> Mostrar la fecha y hora de la última entrada al sistema</p> <p><input checked="" type="checkbox"/> Limite de tiempo permitido en el proceso de log-on</p> <p><input type="checkbox"/> Password no transmitido en texto puro a través de la red</p> <p><input type="checkbox"/> No mostrar la contraseña digitada</p>
11.5.2	<p><b>Identificación y autenticación del usuario</b></p> <p>Tiene el usuario un identificador único para su uso personal</p> <p><input type="radio"/> SI <input checked="" type="radio"/> No</p>
11.5.3	<p><b>Sistema de administración de contraseñas</b></p> <p>Cual de los siguientes elementos no son contemplados por un sistema de administración de contraseñas</p> <p><input type="checkbox"/> Uso individual de ID y password</p> <p><input type="checkbox"/> Tamaño mínimo del password</p> <p><input type="checkbox"/> Forzar al cambio regular del password</p> <p><input checked="" type="checkbox"/> Registro de password ya usados y su reutilización</p> <p><input checked="" type="checkbox"/> Forzar al cambio en el primer log-on</p> <p><input type="checkbox"/> Calidad de las contraseñas</p> <p><input type="checkbox"/> Almacenar y transmitir password de forma cifrada</p> <p><input type="checkbox"/> No mostrar el password en la ventana</p>
11.5.4	<p><b>Uso de utilidades del sistema</b></p> <p>Están controlados y restringidos los utilitarios del sistema que sean capaces de sobrepasar los controles de las aplicaciones o del sistema</p> <p><input type="radio"/> SI <input checked="" type="radio"/> NO <input type="radio"/> No aplicable</p>
11.5.5	<p><b>Terminación de sesión</b></p> <p>Para prevenir el acceso no autorizado de una Terminal, se inactiva la sesión después de un periodo de tiempo de inactividad</p> <p><input type="radio"/> SI <input checked="" type="radio"/> NO</p>
11.5.6	<p><b>Limitación del tiempo de conexión</b></p> <p>Las aplicaciones de alto riesgo, tiene controles de restricciones de horarios de conexión</p> <p><input type="radio"/> SI <input checked="" type="radio"/> NO <input type="radio"/> No aplicable</p>
11.6	<p><b>Control de acceso a las aplicaciones</b></p>

<b>Objetivo</b>	Evitar acceso no autorizado a la información en los sistemas de información
<b>11.6.1</b>	<p><b>Restricción de acceso a la información</b></p> <p>Se emplean los controles de acceso apropiados dentro de los sistemas de aplicación</p> <p><input checked="" type="radio"/> SI <input type="radio"/> No</p> <p>Cuales de los siguientes requerimientos de control de acceso no son contemplados</p> <p><input type="checkbox"/> Acceso controlado a menús</p> <p><input type="checkbox"/> Niveles de acceso controlados</p> <p><input type="checkbox"/> Control de salidas de datos</p> <p><input type="checkbox"/> Restricción de los derechos de acceso</p>
<b>11.6.2</b>	<p><b>Aislamiento de sistemas sensibles</b></p> <p>Son identificados y acordados los riesgos en los que se incurre al ejecutar una aplicación sensible en un ambiente en el cual se comparten recursos</p> <p><input checked="" type="radio"/> SI <input type="radio"/> No <input type="radio"/> No aplicable</p>
<b>11.7</b>	<b>Computación móvil y trabajo remoto</b>
<b>Objetivo</b>	Garantizar la seguridad de la información cuando se usa computación móvil o trabajo remoto
<b>11.7.1</b>	<p><b>Comunicación y computación móvil</b></p> <p>Existe una política para asegurara el debido cuidado al usar computación móvil e instalaciones de comunicación móviles</p> <p><input checked="" type="radio"/> SI <input type="radio"/> No <input type="radio"/> No aplicable</p>
<b>11.7.2</b>	<p><b>Trabajo remoto</b></p> <p>Está todo el trabajo remoto autorizado por la gerencia y específicamente controlado para asegurar el nivel adecuado de protección</p> <p><input checked="" type="radio"/> SI <input type="radio"/> No <input type="radio"/> No aplicable</p> <p>Para el personal involucrado en el trabajo remoto, cual de los siguientes tópicos no son considerados</p> <p><input type="checkbox"/> Seguridad física</p> <p><input type="checkbox"/> Ambiente de trabajo</p> <p><input checked="" type="checkbox"/> Seguridad de las comunicaciones</p> <p><input checked="" type="checkbox"/> Redes inalámbricas</p> <p><input type="checkbox"/> Propiedad intelectual</p> <p><input type="checkbox"/> Licenciamiento de software</p> <p><input type="checkbox"/> Antivirus y firewall</p>