BUENAS PRÁCTICAS EN LA EVALUACIÓN DE SERVICIOS DE TECNOLOGÍA Y DATOS: REPORTES SOC

Junio de 2021

BDO

CONTIGO HOY

VICTOR VERA TUDELA
Socio de Consultoría
BDO Perú

CARLOS ROJAS
Consultor
BDO Perú

BIENVENIDO

- ¿Qué impulsa la evaluación a proveedores que brindan servicios de tecnología & datos?
- ¿Qué reportes de confianza de los servicios externos existen?
- Riesgos que existen al tercerizar las operaciones/servicios de tecnología
- Beneficios obtenidos en una evaluación de organizaciones de servicios de tecnología

- Este webinar está siendo grabando.
- Puede realizar sus preguntas en el panel de Preguntas y Respuestas.

¿QUÉ IMPULSA LA EVALUACIÓN A PROVEEDORES QUE BRINDAN SERVICIOS DE TECNOLOGÍA & DATOS?

¿QUÉ IMPULSA LA EVALUACIÓN A PROVEEDORES QUE BRINDAN SERVICIOS DE TECNOLOGÍA & DATOS?

- Mayor cantidad de servicios que implican el **manejo de datos sensibles** por terceros o usuarios de estos servicios
- **Proliferación de la computación en la nube** que ha generado que más organizaciones externalicen sus servicios
- **Organizaciones con mayor concentración en la esencia de su negocio** y que encargan a especialistas los servicios de tecnología
- Corporaciones, casas matriz, en **búsqueda de eficiencia y cada vez más interconectadas** brindando de sistemas y servicios a sus sedes locales
- Proliferación de clientes que solicitan una **acreditación de los servicios de tecnología** de manejo de datos sensibles
- **Cumplimiento regulatorio** (datos personales) o auditorías externas e internas

¿QUÉ REPORTES DE CONFIANZA DE LOS SERVICOS EXTERNOS EXISTEN?

¿QUÉ REPORTES DE CONFIANZA DE LOS SERVICOS EXTERNOS EXISTEN?

Definiciones de los reportes SOC y tipos

	CONTENIDO	OBJETIVO	INTERESADOS
SOC 1	Evaluación de controles internos relevantes de la organización de servicios que sirven para una auditoría de estados financieros	Auditoría de estados financieros de una organización	• Área de contabilidad / finanzas de la entidad usuaria • Auditores de estados financieros
SOC 2	Evaluación de controles referente al cumplimiento de los criterios de seguridad, disponibilidad, integridad, confidencial y/o privacidad	• Programas de GRC • Supervisión Interna • Debida diligencia • Cumplimiento del proveedor	• Área usuaria • Entes reguladores • Clientes o potenciales clientes
SOC 3	Evaluación de controles referente al cumplimiento de los criterios de seguridad, disponibilidad, integridad, confidencial y/o privacidad	• Marketing • Reputación • Imagen	• Público en general que necesite confiar en los controles de la organización de servicios

RIESGOS QUE EXISTEN AL TERCERIZAR LAS OPERACIONES/SERVICIOS DE TECNOLOGÍA

RIESGOS DE SERVICIOS TERCERIZADOS

1

ACCESO A SISTEMAS E INFORMACIÓN SENSIBLE DE LA EMPRESA POR PERSONAS NO AUTORIZADAS

CONTROL

TODOS LOS REGISTROS, BAJAS Y MODIFICACIONES DE USUARIOS Y PERFILES DE ACCESO DEBEN SER AUTORIZADOS POR EL RESPONSABLE ADECUADO

BDO

RIESGOS DE SERVICIOS TERCERIZADOS

2

USUARIOS ACTIVOS OBTIENEN ACCESO A INFORMACIÓN O FUNCIONALIDADES NO AUTORIZADAS DEL SISTEMA

CONTROL

TODOS LOS ACCESOS LÓGICOS A LOS SISTEMAS ESTÁ ASIGNADO EN FUNCIÓN A UN ANÁLISIS DE SEGREGACIÓN DE FUNCIONES, DE LOS ROLES Y RESPONSABILIDADES DE LOS USUARIOS

BDO

RIESGOS DE SERVICIOS TERCERIZADOS

3

PERSONAS NO AUTORIZADAS QUE MANTIENEN ACCESO A LOS SISTEMAS E INFORMACIÓN DE LA EMPRESA

CONTROL

TODAS LAS CREDENCIALES DE LOS SISTEMAS SE ELIMINAN CUANDO EL ACCESO DEL USUARIO YA NO ESTÁ AUTORIZADO O VENCE EL PLAZO ACORDADO

BDO

RIESGOS DE SERVICIOS TERCERIZADOS

4

MODIFICACIÓN O USO NO AUTORIZADO DE COMPONENTES DE SISTEMAS SIN MEDIDAS DE SEGURIDAD LÓGICAS

CONTROL

IMPLEMENTAR MEDIDAS DE SEGURIDAD LÓGICAS QUE PERMITAN IDENTIFICAR USUARIOS AUTORIZADOS, RESTRINGIR ACCESOS Y DETECTAR ACCESOS NO AUTORIZADOS

BDO

RIESGOS DE SERVICIOS TERCERIZADOS

5

LA INFORMACIÓN DE LOS SISTEMAS SE CORROMPE O SE DESTRUYE, LO CUAL IMPIDE EL CORRECTO FUNCIONAMIENTO DEL MISMO

CONTROL

LA INFORMACION ES RESPALDADA PERIODICAMENTE POR EL ENCARGADO CORRESPONDIENTE, DE ACUERDO A LA POLÍTICA DE RESPALDO DE LA INFORMACIÓN

BDO

RIESGOS DE SERVICIOS TERCERIZADOS

6

LA INFORMACIÓN RESPALDADA ESTÁ CORRUPTA DEBIDO A INCIDENTES, ACTOS MALICIOSOS, DESASTRES NATURALES O ERRORES HUMANOS

CONTROL

LAS COPIAS DE SEGURIDAD SE PRUEBAN PERIÓDICAMENTE PARA ASEGURARSE DE QUE AÚN SE PUEDAN UTILIZAR

BDO

RIESGOS DE SERVICIOS TERCERIZADOS

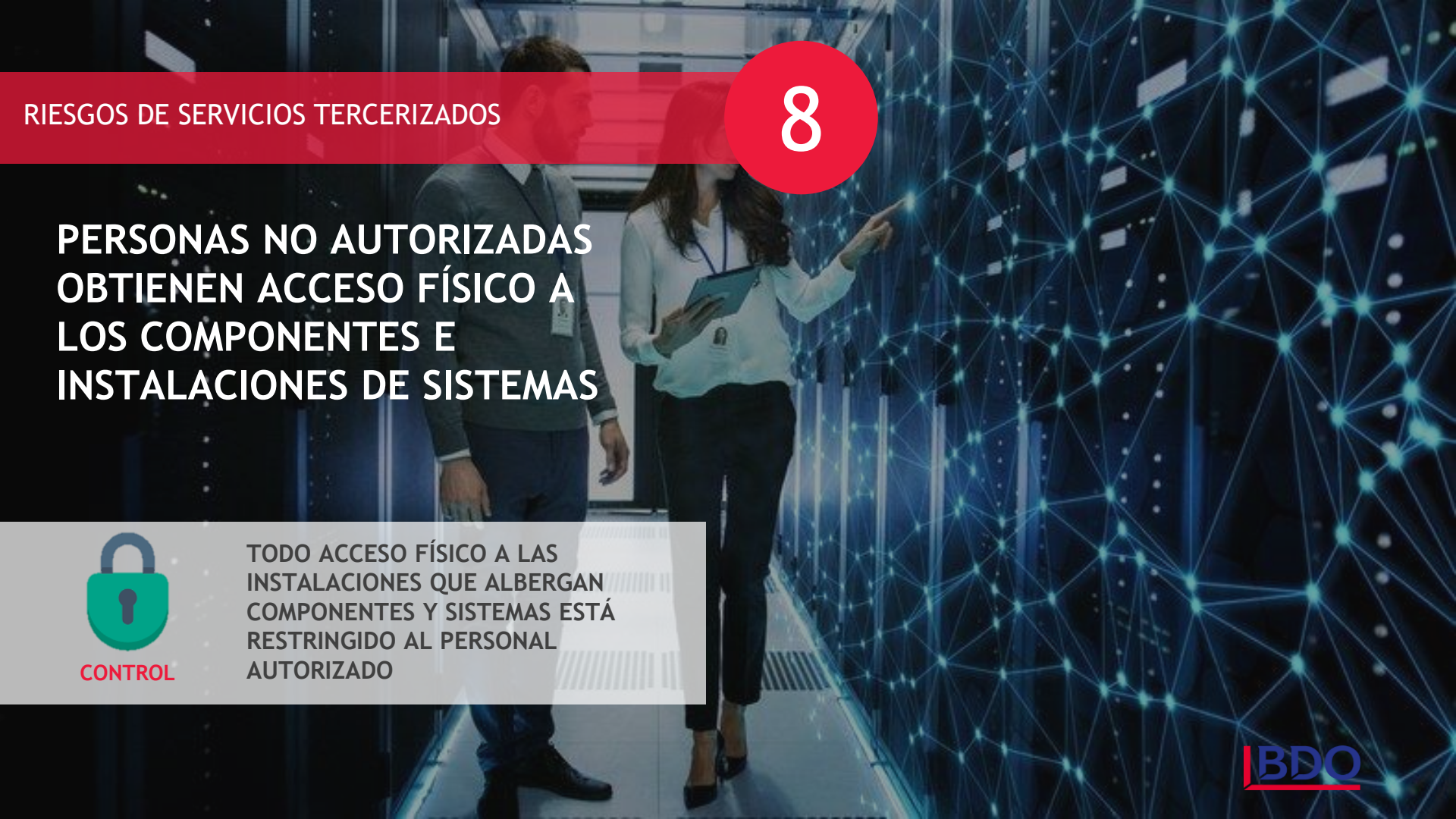
7

VULNERABILIDADES QUE PODRÍAN OCASIONAR UN INCIDENTE NO SON DETECTADOS Y TRATADOS DE MANERA OPORTUNA

CONTROL

SE CUENTA CON PLANES DE RECUPERACIÓN ANTE DESASTRES APROBADOS Y SE PRUEBAN PERIODICAMENTE

BDO



RIESGOS DE SERVICIOS TERCERIZADOS

8

PERSONAS NO AUTORIZADAS OBTIENEN ACCESO FÍSICO A LOS COMPONENTES E INSTALACIONES DE SISTEMAS

CONTROL

TODO ACCESO FÍSICO A LAS INSTALACIONES QUE ALBERGAN COMPONENTES Y SISTEMAS ESTÁ RESTRINGIDO AL PERSONAL AUTORIZADO

RIESGOS DE SERVICIOS TERCERIZADOS

9

DESTRUCCIÓN O ROBO DE CUALQUIER EQUIPO DE TECNOLOGÍA O COMPROMISO DE LA INFORMACIÓN

CONTROL

TODO VISITANTE DEBE CONTAR CON DISTINTIVO QUE ACREDITE SU IDENTIDAD Y QUE PERMITA EL ACCESO SOLO A LAS ÁREAS AUTORIZADAS Y EQUIPOS DE TECNOLOGÍA

BDO

RIESGOS DE SERVICIOS TERCERIZADOS

10

UNA PERSONA ANTERIORMENTE AUTORIZADA OBTIENE / MANTIENE ACCESO A LAS INSTALACIONES DE TECNOLOGÍA

CONTROL

EJECUTAR REVISIONES PERIÓDICAS DE LA LISTA DE ACCESO FÍSICO DEL PERSONAL E IDENTIFICAR ACCESOS OTORGADOS A PERSONAS CESADAS DE LA EMPRESA

BDO

RIESGOS DE SERVICIOS TERCERIZADOS

11

CAMBIOS EN LOS SISTEMAS NO AUTORIZADOS POR LOS RESPONSABLES Y SIN TRAZABILIDAD

CONTROL

TODOS LOS CAMBIOS DE LOS SISTEMA SE AUTORIZAN, DISEÑAN, DESARROLLAN, CONFIGURAN, DOCUMENTAN, PRUEBAN E IMPLEMENTAN DE ACUERDO CON LOS COMPROMISOS Y REQUISITOS

BDO

12

ATAQUE EXTERNO DE SEGURIDAD, INFECCIÓN MASIVA DE RECURSOS QUE CONDUCE A UNA INTERRUPCIÓN NO PLANIFICADA DE LOS SERVICIOS

CONTROL

SE EJECUTAN PERIÓDICAMENTE ANÁLISIS DE PENETRACIÓN Y LAS EVALUACIONES DE VULNERABILIDAD DE LA RED INTERNA Y EXTERNA, Y DEFINICIÓN DE ACCIONES CON LA AUTORIZACIÓN DE LA DIRECCIÓN

BENEFICIOS OBTENIDOS EN UNA EVALUACIÓN DE ORGANIZACIONES DE SERVICIOS DE TECNOLOGÍA

BENEFICIOS OBTENIDOS EN UNA EVALUACIÓN SOC

CONFIANZA DE NUESTROS CLIENTES

APORTE AL NEGOCIO

PUBLICAR EL REPORTE SOC PARA AFIANZAR LA CONFIANZA DE LOS STAKEHOLDERS EN NUESTROS SERVICIOS DE TECNOLOGÍA

BDO

BENEFICIOS OBTENIDOS EN UNA EVALUACIÓN SOC

FORTALECIMIENTO DEL CONTROL INTERNO

APORTE AL NEGOCIO

REDUCIR EL IMPACTO DE LAS AUDITORÍAS INTERNAS DE LOS PROCESOS DE TECNOLOGÍA

BDO

BENEFICIOS OBTENIDOS EN UNA EVALUACIÓN SOC

MITIGACIÓN DE RIESGOS

APORTE AL NEGOCIO

GESTIÓN ADECUADA DE RIESGOS ASOCIADOS A TECNOLOGÍA CON LA EVALUACIÓN DE LOS CONTROLES CORRESPONDIENTES

BDO

BENEFICIOS OBTENIDOS EN UNA EVALUACIÓN SOC

ESTANDARIZACIÓN DE SERVICIOS TERCERIZADOS

APORTE AL NEGOCIO

ASEGURAR QUE NUESTROS PROCESOS DE TECNOLOGÍA SIGUEN BUENAS PRÁCTICAS BASADO EN ESTANDARES INTERNACIONALES

BDO

BENEFICIOS OBTENIDOS EN UNA EVALUACIÓN SOC

SERVICIOS DE TECNOLOGÍA CONFIABLES

APORTE AL NEGOCIO

ENCARGAR A ESPECIALISTAS LA ADMINISTRACIÓN DE NUESTROS SERVICIOS DE TECNOLOGÍA

BDO

PREGUNTAS Y RESPUESTAS

¡GRACIAS POR SU PARTICIPACIÓN!

Somos líderes en servicio excepcional al cliente

VICTOR VERA TUDELA
Socio de Consultoría
BDO Perú
vveratudela@bdo.com.pe

CARLOS ROJAS
Consultor
BDO Perú
crojasr@bdo.com.pe

Síguenos en:

www.bdo.com.pe

¡Gracias!

BDO Consulting S.A.C., una sociedad anónima cerrada peruana, es miembro de BDO International Limited, una compañía limitada por garantía del Reino Unido, y forma parte de la red internacional BDO de empresas independientes asociadas. BDO es el nombre comercial de la red BDO y de cada una de las empresas asociadas de BDO.