DGGRAI Fundación de la Universidad del Valle de Guatemala
Dirección General de Gestión de Riesgos y Auditoría Interna
Auditoría Interna | Gestión de Riesgos | Consultoría | Auditoría Externa | Seguros

No.
09-2017
Septiembre

En este boletín:

Seguridad de los datos

¿Sabe qué tan factible es que pueda perder la información? Este es un tema que está ganando auge en los últimos años, por lo que es importante saber por dónde empezar.

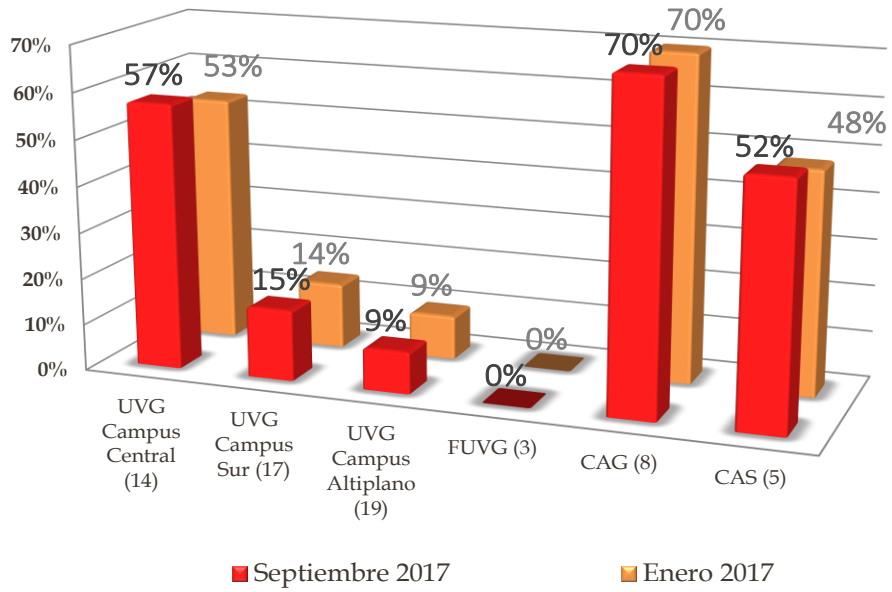
Visita de trabajo

En el mes de Septiembre se realizó una visita de una semana a UVG Campus Altiplano, con el propósito de trabajar con los distintos Directores del Campus, buscar acercamiento, resolver dudas y continuar con el avance de las matrices de riesgos.

Adicionalmente se realizó inducción a la Fase I del proceso de Gestión de Riesgos, a las unidades de Registro Académico y Ayudas Financieras para que continúen con la construcción de la matriz de riesgos de dichas unidades, por lo que desde ya les deseamos éxitos.

Si usted desea una capacitación, taller o charla para su equipo de trabajo, en donde considere que podemos ayudarle, comuníquese con nosotros.

Gráfica de avance de la Gestión de Riesgos



Nota

El parámetro de medición del porcentaje de avance es la fase concluida, por lo que no se consideran unidades que tengan fases incompletas aunque estén por terminar. El número que se encuentra entre paréntesis es la cantidad de unidades por campus que ya está trabajando matrices de riesgo.

Las columnas en color naranja corresponden al avance hasta Enero 2017, las columnas de color rojo representan el avance a Septiembre 2017.

Seguridad de los datos

Introducción

Los datos son uno de los activos más valiosos que una institución tiene a su disposición, y abarcan todo, desde estrategias, mallas curriculares, transacciones financieras hasta registro de los clientes (estudiantes), proveedores, etc.

Sin embargo, hoy en día existe el "riesgo digital" pues para bien o para mal el avance tecnológico también trae a los ataques cibernéticos que han llegado para quedarse. A continuación se presentan algunos pasos para mejorar la seguridad de los datos.

1. Conozca dónde se encuentran sus datos.

Comprender qué datos tiene, dónde están, quién es responsable y quién tiene acceso a ellos es fundamental para construir una buena estrategia de seguridad. De acuerdo al sistema de almacenamiento que utilice, así debe ser el tipo de protección que requiere la información: discos locales, sistemas de respaldo basados en disco, en cintas fuera de las instalaciones y en la nube.

2. Construya una política de "conocimiento según necesidad".

Para minimizar el riesgo del error humano (o curiosidad), cree políticas que limiten el acceso a datos particulares. Internamente categorice la información y determine qué información puede ser de acceso público y cuál sería de acceso restringido.

Mantener controles sobre quién puede acceder a los datos y qué datos se pueden obtener es extremadamente importante.

3. Monitoree el ciclo de vida de los datos.

Identificar los datos que debe proteger, y por cuánto tiempo; tener en cuenta las consecuencias que tendría la pérdida de esos datos.

4. Evaluar riesgos de datos

Evaluar cualquier peligro potencial para la información, desde una violación de datos en línea, cortes de energía, sabotaje, etc. Esto le permitirá identificar cualquier punto débil de la seguridad y formular un plan sobre cómo remediarlo y priorizar las acciones para reducir el riesgo de una fuga de datos.

5. Realizar copias de seguridad regulares

Es importante realizar respaldos a una frecuencia acorde a las necesidades de la unidad. Asegúrese que institucionalmente se está realizando una copia de los datos de la unidad.

6. Capacitar al personal

Es importante que cada colaborador comprenda los riesgos y consecuencias de las violaciones de datos y saber cómo prevenirlas. Considere temas asociados a enlaces malware, spam, notificaciones cuando la computadora funciona de forma extraña, etc.

Si perdiera los datos, ¿sabe con exactitud qué recuperar?

Conclusión

Ante las amenazas del mundo digital, es indispensable tomar medidas para la protección de los datos, por lo cual se recomienda construir y mantener un registro de ellos, dónde se almacenan, quién es el responsable de los mismos, qué accesos existen y las medidas de seguridad que se tienen.

Considerar la creación de un programa de formación del personal, para asegurar que todos son conscientes de la importancia de la información con la que están tratando y la necesidad de utilizarla de forma segura.

Referencias

[1] *Ashford, Farrera, Granneman, Phifer, Sales, Vicente.;* (2016). Consejos de ciberseguridad para las empresas de hoy, TechTarget Inc., Newton, MA. 11-17 pp.

[2] *Andrews, C.* (2017). Seis procesos esenciales para mantener los datos seguros. Disponible en: http://searchdatacenter.techtarget.com/es/opinion/Seis-procesos-esenciales-para-

Contáctenos

17av. 10-97 zona 15, Vista Hermosa III. Guatemala, C.A.
Tel. (502) 2507-1500 ext. 21338 y 21339

E-mail:

Orlando Pineda Vallar:
fopineda@uvg.edu.gt

Catalina González:
cgonzalez@uvg.edu.gt