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. 03-2017

EN ESTE BOLETÍN:

SEGURIDAD DE LA INFORMACIÓN

Qué pasaría si: ¿Un importante contrato fuera sustraído de su oficina? ¿Alguien decide sabotearlo y borra una base de datos valiosa?

"Somos el cambio que queremos ver en el mundo."

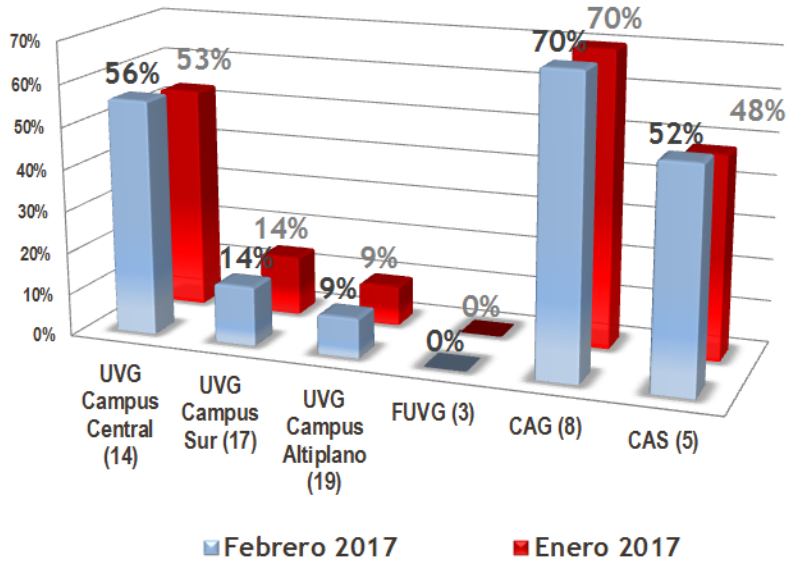
MAHATMA GANDHI

PROGRAMA DE CAPACITACIONES

Como parte de nuestro Plan de Prevención, en el mes de febrero realizamos el taller "Herramientas para construcción y análisis de procesos" en UVG Campus Sur, Colegio Americano del Sur y UVG Campus Altiplano, con la participación de colaboradores y directores de las distintas unidades.

Agradecemos el apoyo recibido por las Direcciones Ejecutivas y Administrativas en la coordinación de estos talleres.

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.

AVANCES DE LA GESTIÓN DE RIESGOS EN EL GEV

Hacemos extensiva la felicitación al **Departamento ITS (Information & Technology Services) del Colegio Americano del Sur,** que ha concluido satisfactoriamente el trabajo de la Fase I de la metodología de Gestión de Riesgos.

Así mismo, queremos reconocer el trabajo realizado por el **Departamento de Cuentas por Cobrar de la Universidad del Valle de Guatemala Campus Central,** que concluyeron satisfactoriamente las Fases IV y V. Por lo que ha terminado un ciclo completo del proceso de Gestión de Riesgos.

SEGURIDAD DE LA INFORMACIÓN

Introducción

A través del tiempo se han visto cambios drásticos en la forma en la que nos comunicamos, eso ha generado un cambio en la forma en que se presenta la información y con ello, las vulnerabilidades y amenazas que contiene.

Conocer esas amenazas nos permite prepararnos para resguardar información que se considere valiosa o confidencial, y a garantizar su disponibilidad e integridad.

Las amenazas

Pueden ser tan simples e inocentes como derramar agua accidentalmente en una computadora, o bien un ataque premeditado y dirigido, como lo sería la manipulación o alteración no autorizada de información. En cualquiera de los casos, puede ser hacia información física o digital, por lo que requieren de nuestra atención y acción.

A continuación se describen las amenazas más comunes:

1. Fuego
2. Daño por agua
3. Humedad de los ambientes
4. Hurto o Robo de información.
5. Sabotaje.
6. Suplantación de identidad de usuario.
7. Acceso no autorizado a áreas restringidas.
8. Destrucción premeditada de la información.
9. Divulgación de la información.
10. Ingeniería social.
11. Extorsiones.

Otras amenazas se describen en el siguiente link:
Amenazas a la seguridad de la información.

Fuente: www.ISO27000.es

Medidas que se pueden tomar

Lo ideal es la existencia de una política de seguridad de la información, sin embargo, internamente se pueden tomar ciertas medidas para disminuir la vulnerabilidad de la información a las amenazas:

Identifique los riesgos reales: Determine cuál es la información más importante de su unidad, dónde está ubicada y quién tiene acceso. Evalúe si las condiciones actuales representan un riesgo real.

Proteja lo más importante: Es virtualmente imposible eliminar las amenazas, sin embargo, mejorar las condiciones ayuda a disminuir la vulnerabilidad. Dentro de esas mejoras podría incluirse: Ajustar la forma en la que se comparte la información; concientizar al equipo de trabajo de los peligros existentes; apoyarse en servicios que la institución ya tiene a su disposición para detectar algunas deficiencias (back up, cajillas de seguridad, Auditoría interna, Gestión de riesgos, Departamento de seguridad, etc.).

"La clave para tener un entorno más seguro es lograr que sus empleados entiendan su responsabilidad personal al momento de utilizar nuevas tecnologías o tener acceso a información corporativa. Esta concientización va más allá de las políticas de alto nivel e incluye ejemplos pragmáticos, como las actividades permitidas y prohibidas al momento de utilizar redes sociales, laptops, tabletas o teléfonos inteligentes. Una lista concreta de "lo que debe y no debe hacerse" es la forma más eficaz de comunicar las políticas y habilitar su uso responsable."(1:12)

CONCLUSIONES:

Puede hacer algunas preguntas para lograr un entendimiento general: ¿Cuál es la información que a su criterio podría estar amenazada o en peligro?, ¿Identifica alguna amenaza dentro o fuera de la unidad/institución?, ¿Es posible hacer algo al respecto?, ¿Puede apoyarse con otras unidades para prevenir?, ¿Debería reportar la vulnerabilidad identificada a su superior?

Referencias

[1] Ernst & Young, (2011) *Seguridad de la información en un mundo sin fronteras.* México. Ernst & Young Global. 16pp.

[2] *Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información;* (2005). COGUANOR NTG/UNIT/ISO/IEC 27002:2005. 167pp.

[3] Guía para empresas: Cómo adaptarse a la normativa sobre protección de datos. (2009). INTECO. Instituto Nacional de Tecnologías de la Comunicación. España. INTECO. 68pp.

Contáctenos

17av. 10-97 zona 15, V. H. III.
Tel. (502) 2507-1500 ext. 21338 y 21339

E-mail:

Orlando Pineda Vallar:
fopineda@uvg.edu.gt
Catalina González:
cgonzalez@uvg.edu.gt