Controles y auditoría en la identidad digital

Author : a.h.

Categories : Auditoría, Certificación y Calidad de Sistemas Informáticos

Date : 25 noviembre, 2018

Para esta cuarta entrega de este fascinante tema, que no es otro que la identidad digital, voy a abordar los controles y auditorias que se pueden implantar para la gestión de riesgos. En el post anterior traté de mostrar los 5 mayores riesgos que tiene hoy en día el área que me compete, pero para contrarrestar estos peligros existen unas estrategias que deben ser implementadas en las organizaciones. La primera tanda de medidas se centran en tratar de prevenir que los riesgos sean materializados [1].

1. Definir estrategia de identidad corporativa. Para mantener una buena reputación online a nivel organizacional, se debe de tener una estrategia previa bien definida que contemple qué se desea transmitir. Se deben definir los objetivos en materia de identidad digital, diseñar una imagen de marca y seleccionar un nombre de dominio adecuado a su denominación social o marca. Además, se debe proteger este dominio con las herramientas existentes dentro de la propiedad intelectual e industrial para evitar el riesgo número 4 presentado en el post anterior (Registro abusivo del nombre de dominio). Para lograr esto se debe designar a un *Community Manager* y emplear los recursos materiales y humanos que sean necesarios.
2. Interacción con los usuarios. Hoy en día la interacción con los usuarios en un entorno como Internet es algo esencial para una empresa pero se debe tener en cuenta que esta comunicación expone a la organización a críticas que pueden ser muy perjudiciales. Es por ello que se debe definir qué modelos comunicativos se van a usar y reflexionar sobre cuestiones como las siguientes:
    1. ¿Qué tono se va a utilizar en la interacción? (amigo, experto,...)
    2. ¿En qué tipo de casos se va a responder a los usuarios?¿De forma pública, privada y/o personalizada?
3. Redes sociales. En este punto rescato el papel del *Community Manager* como parte fundamental a la hora de gestionar la identidad digital de una organización. El problema surge con el uso de estas redes por parte de los trabajadores de la entidad. Es por ello

que en este punto se plantea la creación de una política interna de uso de redes sociales. En ella se establecen recomendaciones y obligaciones para hacer un buen uso de tan peligrosas redes y evitar así el riesgo número 5 del post anterior (fuga de información). Además se puede complementar esta política con un manual de buenas prácticas que aborde puntos como:
    1. Se debe cambiar la contraseña cada un determinado tiempo y no reutilizar claves de otros servicios.
    2. Si no se dispone de la autorización de la compañía, no dar a entender en RRSS que se habla en nombre de la misma.
    3. Se debe evitar criticar productos de la competencia de manera irresponsable.
    4. Se debe evitar entrar en debate con potenciales clientes.
4. Cumplimiento normativo. Es esencial cumplir con las normativas existentes en el sector que desempeñe la entidad su labor pero además debe de tenerse siempre en cuenta la RGPD como base para no infringir los derechos de los ciudadanos europeos en cuanto a protección de datos.
5. Implantar medidas de seguridad. Para tratar de evitar ciberataques es importante que las empresas estén preparadas. Para ello se deberían contemplar escenarios de crisis y procedimientos de respuesta como notificaciones de brechas de seguridad o de atención a peticiones. También es imprescindible contar con sistemas de recuperación ante desastres que no permitan que la identidad digital de la corporación se vea comprometida.

Pero todas estas medidas solo tratan de reducir la probabilidad de que el riesgo se materialice. Como ya he comentado anteriormente, el riesgo 0 no existe y por lo tanto, además de prevenir, debemos tener una hoja de ruta de qué hacer si algo ocurre. A continuación se adjunta en formato imagen un patrón orientativo realizado por INCIBE (Instituto Nacional de Ciberseguridad) que puede modificarse adecuándose al sector de la organización [2].

Además, me gustaría hacer referencia a un ppt muy interesante de buenas prácticas en el ámbito de la identidad digital creado por *KnowledgeLeader* que plantea una hoja de ruta para gestionar tan importante área [3].

En el próximo y último post abordaré este tema desde una perspectiva diferente a la actual y trataré de predecir qué va a ocurrir con la identidad digital en los próximos años.

---

[1] “Identidad digital: la reputación online de las empresas”, acceso el 24 de noviembre de 2018. https://www.incibe.es/protege-tu-empresa/blog/infografia-id-empreas

[2] “Ciberseguridad en la identidad digital y la reputación online”, acceso el 24 de noviembre de 2018. https://www.incibe.es/extfrontinteco/img/File/empresas/guias/guia_ciberseguridad_identidad_online.pdf

[3] “Identity and access management - Best Practices Guide”, acceso el 24 de noviembre de 2018. https://www.knowledgeleader.com/knowledgeleader/content.nsf/web+content/guidentityandaccessmanagementbestpracticesguide?