CLUB EXCELENCIA EN GESTIÓN

CLUB DE EVALUADORES

Aspectos prácticos para la evaluación de la Ciberseguridad con el nuevo Modelo EFQM

#compartiendoymejorando

18 de junio de 2020

Ahora más que nunca, compartiendo y mejorando

Xavier Rubiralta Costa

- Evaluador Senior EFQM, del Premio Europeo, Iberoamericano y de más de 25 sellos EFQM
- Licenciado en Informática (UAB 1985) y Master en Seguridad Informática (UOC 2006)
- Profesional de las Tecnologías de la Información desde 1981, los últimos 18 años focalizado en ciberseguridad, privacidad, gestión de riesgos y gobierno de TI
- Responsable de proyectos de ciberseguridad en la UAB
- Vocal del Comité Técnico de Normalización 320 de UNE: Ciberseguridad y protección de datos personales
- Profesor a tiempo parcial en UOC, UAB, ICAB, UVic-UCC
- Miembro asociaciones profesionales: Colegio Ingeniería Informática (Junta), ISACA (Junta), ISC2 (SME), etc
- Certificaciones profesionales del ámbito de TI

CLUB DE EVALUADORES

CLUB EXCELENCIA EN GESTIÓN

Aspectos prácticos para la evaluación de la ciberseguridad con el nuevo modelo EFQM

- Reflexiones previas
- Contextualizar la organización
- Elementos clave de la ciberseguridad
- Aspectos a considerar en la evaluación
- Desarrollo de la evaluación
- COVID-19
- Referencias

Reflexiones previas

- ¿Tiene asegurada la sostenibilidad una organización con una débil gestión de la ciberseguridad?
- ¿Es importante la ciberseguridad en una evaluación?
- ¿Puede ser sobresaliente una organización sin gestionar bien la tecnología?
- Visión holística y no solo tecnológica
- Tecnología = oportunidades + riesgos

Reflexiones previas:

Ubicación en el modelo

- Propósito, visión y estrategia
- Cultura de la organización y liderazgo
- Implicación de los grupos de interés (GI)
- Crear valor sostenible
- Gestionar el funcionamiento y la transformación
- Percepción de los GI
- Rendimiento estratégico y operativo

CLUB DE EVALUADORES

CLUB EXCELENCIA EN GESTIÓN

Reflexiones previas:
Ubicación en el modelo

Gestionar el funcionamiento y la transformación:

- Gestionar el funcionamiento y gestionar los riesgos
- Transformar la organización de cara al futuro
- Gestionar la innovación y utilizar la tecnología
- Potenciar datos, información y conocimiento
- Gestionar activos y recursos

CLUB DE EVALUADORES

CLUB EXCELENCIA EN GESTIÓN

Contextualizar la organización

- Importancia de la tecnología en la organización: en la estrategia, en las operaciones, y en los productos y servicios
- LA TECNOLOGÍA DEBE SER SEGURA Y CONFIABLE
- Sector de actividad
- Tipos de datos e información con la que se opera
- Perfiles profesionales y nivel de competencia digital
- Tecnologías de la Información (TI) y Tecnologías de las Operaciones (TO): automatización robótica de procesos (RPA), Industria 4.0, Internet de las Cosas (IoT), etc
- Internacionalización: entornos de trabajo y legislaciones

Contextualizar la organización

- Cadena de suministros y terceras partes
- Compliance: RGPD, Esquema Nacional de Seguridad (ENS), Directiva NIS (Seguridad en Redes y Sistemas de Información), etc
- Las sanciones del RGPD pueden llegar al 4% volumen negocio anual
- Legislaciones específicas (Infraestructuras Críticas, SOX, etc)
- Forensic Readiness (preparar evidencias para litigios, etc)
- Paradigmas tecnológicos relevantes
- Cloud (servicios en la nube)
- Movilidad, teletrabajo, ¿aún existe el perímetro?
- Seguridad física: protección de dispositivos

Elementos clave de la ciberseguridad

- Evolución: seguridad informática, seguridad de la información y ciberseguridad
- Dimensiones: CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD, trazabilidad y autenticidad (no repudio)
- Confidencialidad: propiedad intelectual y privacidad (datos personales y categorías especiales de datos)
- Medidas de protección: PERSONAS, PROCESOS y TECNOLOGÍA
- Rol del CISO (Chief Information Security Officer), Responsable de Ciberseguridad o Responsable de Seguridad de la Información

Elementos clave de la ciberseguridad

Análisis de riesgos

- Riesgo = Probabilidad x Impacto
- Amenazas y Vulnerabilidades
- Proteger los activos (información) en función del valor y del riesgo
  Análisis coste-beneficio
- Tratamientos: mitigar, eliminar, transferir o aceptar
- Gestión integrada de todos los riesgos o gestión aislada de los riesgos tecnológicos
- ISO 31000
- Tipos de riesgos, entre otros, reputacionales, de incumplimiento, etc
- Riesgo residual

Elementos clave de la ciberseguridad

- Gestión de incidentes de ciberseguridad. Escalado. Obligación de informar. Registro de incidentes. ¿Los ha habido?
- Incidentes en la protección de datos de carácter personal (72 horas)
- Securización del puesto de trabajo
- BYOD (Bring Your Own Device): propiedad del dispositivo desde el que se trabaja
- Redes inalámbricas
- Metodologías ágiles versus gestión del cambio robusta en los entornos de producción
- Identificación, autenticación, autorización y trazabilidad
- Factores de autenticación: algo que sé, algo que tengo y algo que soy (biometría). Autenticación fuerte: más de un factor

Elementos clave de la ciberseguridad

Plan de Continuidad de Negocio (BCP) (ISO 22301) / Plan de Recuperación de desastres (DRP) / Plan de contingencias

- BIA (Business Impact Analysis): funciones críticas para el negocio
- RTO (Recovery Time Objective): tiempo máximo que puede estar no disponible una función crítica
- RPO (Recovery Point Objective): punto desde el que se han de poder recuperar los datos, es decir, cuantos datos se pueden perder

Gobierno de TI (ISO 38500 y COBIT): 4 pilares: alineación estratégica, aportación de valor, gestión de riesgos y gestión de recursos

- Alineación de los objetivos de ciberseguridad (y de TI) con la estrategia corporativa

Aspectos a considerar en la evaluación

¿Está formalizada la ciberseguridad?

- Plan de ciberseguridad o de seguridad de la información
- Plan de Tecnologías de la Información (TI)
- Política de seguridad, ciberseguridad, seguridad de la información o seguridad integral
- Normativas (por ejemplo de trabajo remoto)
- Procedimientos (por ejemplo de configuración del correo electrónico en un dispositivo móvil concreto)
- Nombramiento del responsable de ciberseguridad (CISO)

Aspectos a considerar en la evaluación

- Certificaciones (ISO 27001). Alcance
- Auditorías realizadas (de cumplimiento ENS, etc)
- ¿Quién gestiona la ciberseguridad? ¿Dónde está el conocimiento? Proveedores externos. Formalización de los acuerdos de nivel de servicio (SLA)
- Alianzas en ciberseguridad y alianzas en TI
- Gestión del talento en ciberseguridad (bien escaso)
- Vigilancia tecnológica en el ámbito de la ciberseguridad
- Ubicación, estructura y recursos de la unidad de ciberseguridad
- ¿Cuáles son los referentes? Normas, organismos, proveedores externos, centros de formación, comparaciones, etc

CLUB DE EVALUADORES

CLUB EXCELENCIA EN GESTIÓN

Aspectos a considerar en la evaluación

- Concienciación (universal). Personal externo
- Formación: especialistas, técnicos, líderes, etc
- Gestión de identidades. Credenciales de personal externo. Trazabilidad. Credenciales de uso compartido
- Shadow IT: información gestionada en herramientas que el departamento de TI “ignora” y “se escapan a su control”
- Data Loss Prevention (DLP): prevención de fuga de datos
- Fraude interno: medidas de prevención, monitorización y medición
- Ciberseguros
- Relación CISO y DPD/DPO (Delegado de Protección de Datos)
- Relación entre las funciones de seguridad física y ciberseguridad
- Política de uso de redes sociales

Desarrollo de la evaluación

¿A quién preguntar?

- Líderes
- Responsables de negocio / áreas funcionales
- Recursos Humanos
- Legal
- Control Interno
- Departamento de TI
- Ciberseguridad
- Focus groups
- Observación de campo

Desarrollo de la evaluación

- Buscar lenguaje común y facilitador. Utilizar diferentes registros

¿Han sido víctimas de …?

- Ramsomware / Infecciones de código maligno
- Ingeniería social / Phishing
- Ataques de denegación de servicio (DDoS)
- SPAM (correo indeseado)
- Robo de credenciales y fugas de datos
- Ataques a webs
- ¿Cuál ha sido el incidente más grave? Lecciones aprendidas y medidas de protección derivadas

Desarrollo de la evaluación

- ¿Cómo se detectan comportamientos anómalos?
- Correlación de eventos y ciberinteligencia
- ¿Hay límites en la navegación de los empleados?
- ¿Pueden los empleados instalar programas en su puesto de trabajo?
- ¿Cómo se asegura la ciberseguridad en terceras partes?

Mejoras en el ámbito de la ciberseguridad desde la última evaluación:

- En las personas
- En los procesos y procedimientos
- En medidas tecnológicas

Desarrollo de la evaluación

Indicadores:

- Infecciones, interrupciones de servicio, suplantación de identidad, etc
- Indicadores de terceras partes que afectan a la organización
- Medición del impacto económico de los incidentes
- ¿Quién los utiliza? Líderes, responsables de negocio, etc
- Relación de los indicadores con la estrategia corporativa
- Comparativas
- ¿Hay medidas de percepción de la ciberseguridad por parte de los clientes? ¿De los empleados? ¿De otros grupos de interés? ¿Cómo de obtienen?

Desarrollo de la evaluación

Excelencia en la gestión de la ciberseguridad (y de TI)

- Implicación en el modelo. ¿Qué aporta a éste al ámbito?

Cumplimiento en el ámbito de ciberseguridad (y de TI)

- Medición del grado de cumplimiento. Planes de mejora pendientes. Impacto de no cumplimiento

Ética en el ámbito de la ciberseguridad (y de TI)

- Uso ético de la tecnología y en concreto de la inteligencia artificial
- Equilibrio entre derechos individuales versus riesgos colectivos o de la organización

COVID-19

- Lecciones aprendidas y planes de mejora derivados
- Incidentes acaecidos
- ¿Cómo de bien preparados estábamos?
- Evolución de indicadores (antes y después). Variaciones en los datos y en los sistemas de medición
- Recogida de datos de salud (PRL). Reconocimiento facial

Cambios en el teletrabajo:

- Personas
- Procesos y procedimientos
- Plataformas y herramientas tecnológicas

Referencias

Nomas de referencia:

- ISO 27001 Sistema de Gestión de Seguridad de la Información
- ISO 22301 Sistema de Gestión de la Continuidad de Negocio
- ISO 31000 Gestión del riesgo. Principios y directrices
- ISO 20000 Gestión de servicios. Requisitos del Sistema de Gestión de Servicios
- NIST SP 800-53 Controles de seguridad y privacidad para los sistemas de información federales de EEUU
- NIST SP 800-34 Contingency Planning Guide for Federal Information Systems

Referencias

Decálogo Ciberseguridad Empresas

Instituto Nacional de Ciberseguridad (INCIBE)

https://www.incibe.es/protege-tu-empresa/guias/decalogo-ciberseguridad-empresas-guia-aproximacion-el-empresario

CLUB DE EVALUADORES

CLUB EXCELENCIA EN GESTIÓN

Referencias

BALDRIGE CYBERSECURITY EXCELLENCE BUILDER

Herramienta de autoevaluación propuesta por el National Institute of Standards and Technology (NIST) que permite analizar la madurez de la gestión de la ciberseguridad de una organización e identificar oportunidades de mejora. Éstas originarán planes de acción y las sucesivas autoevaluaciones permitirán observar el progreso en la ciberseguridad.

Combina la ciberseguridad con la visión del modelo americano de excelencia en gestión (Baldrige) y estructura el amplio cuestionario según este modelo. El hecho que el modelo de excelencia se implique en la definición de las cuestiones clave en la evaluación de la ciberseguridad, es una evidencia de la importancia de ésta para cualquier organización desde un punto de vista de la alta dirección.

https://revistasic.es/revista-sic/sic-131/colaboraciones/evaluacion/

CLUB DE EVALUADORES

CLUB EXCELENCIA EN GESTIÓN

Referencias

Glosario de términos de ciberseguridad: una guía de aproximación para el empresario - INCIBE

https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridad-guia-aproximacion-el-empresario

Guía de Seguridad (CCN-STIC-401) Glosario y abreviaturas - Centro Criptológico Nacional

https://www.ccn-cert.cni.es/guias/glosario-de-terminos-ccn-stic-401.html

Glosario de terminología TIC – Consejo General Abogacía Española

https://www2.abogacia.es/publicaciones/ebooks/glosario-terminologia-tic/

Glossary of Key Information: Security Terms - National Institute of Standards and Technology

https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Referencias

Si necesitas teletrabajar sigue estos consejos de seguridad - INCIBE

https://www.incibe.es/protege-tu-empresa/blog/si-necesitas-teletrabajar-sigue-estos-consejos-seguridad-0

CCN-CERT BP/18 recomendaciones de Seguridad para situaciones de teletrabajo y refuerzo de vigilancia - Centro Criptológico Nacional

hhttps://www.ccn-cert.cni.es/cibercovid19/teletrabajo.html

Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo - Agencia Española de Protección de Datos

https://www.aepd.es/sites/default/files/2020-04/nota-tecnica-proteger-datos-teletrabajo.pdf

Guide to Enterprise Telework, Remote Access and Bring Your Own Device (BYOD) Security – National Institute of Standards and Technology

https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final

CLUB DE EVALUADORES

CLUB EXCELENCIA EN GESTIÓN

Referencias

Ciberseguridad vista desde el prisma EFQM

http://www.agoraceg.org/banco-conocimiento/cybersecurity-seen-through-prism-efqm-ciberseguridad-visto-desde-el-prisma-efqm

GDPR: A new privacy framework to align with EFQM

http://www.agoraceg.org/banco-conocimiento/gdpr-new-privacy-framework-align-efqm

La gestión de la información y la ciberseguridad, claves para la excelencia

http://www.agoraceg.org/blog/la-gestion-de-la-informacion-y-la-ciberseguridad-claves-para-la-excelencia

EFQM and IT Governance

http://www.agoraceg.org/banco-conocimiento/efqm-and-it-governance

FORMACIÓN
TRANSFORMACIÓN EVALUADORES EFQM
TRES ÚLTIMAS CONVOCATORIAS
ONLINE EN DIRECTO

- **1 y 2 de julio de 2020 COMPLETO**
- **29 y 30 de septiembre de 2020 4 últimas plazas**
- **18 y 19 de noviembre de 2020**

Información e inscripciones en

www.clubexcelencia.org

CLUB DE EVALUADORES

CLUB EXCELENCIA EN GESTIÓN

Próximos webinars exclusivos del Club de evaluadores

Evaluación de estrategias ágiles en entornos VUCA

Laura Cuello. EFICIL

2 de julio a las 12.00h.

Los Objetivos de Desarrollo Sostenible y el Modelo EFQM 2020

Joan Ramón Dalmau. ADDERE Consulting Group

10 de julio a las 12.00 h

Información e inscripciones en

ÁGORA CEG

CLUB DE EVALUADORES

CLUB EXCELENCIA EN GESTIÓN

#LoEstamosConsiguiendo

CLUB DE EVALUADORES

CLUB EXCELENCIA EN GESTIÓN

Compartiendo y mejorando juntos

www.clubexcelencia.org

Club excelencia en Gestión

Club excelencia en Gestión

@Club_excelencia

Canal Club excelencia en Gestión

@club_excelencia

CLUB EXCELENCIA EN GESTIÓN

Este documento ha sido adquirido por . Las copias o reenvíos infringen el copyrigth.

Por favor, diríjase a la web del Club Excelencia en Gestión (www.clubexcelencia.org) si está interesado en obtener una copia.