VALVONTA

Auditoria y Seguridad

www.valvonta.es

INtroducción

IN – INNOVACION, INSPIRACION, INTUICION

I. Comprometidos con la Seguridad de la Informacion en todos sus aspectos. Desde la continuidad de negocio a la conservación de la información en soporte digital.

II. Expertos en adecuar procedimientos para que la digitalización integra del negocio no este comprometida y sea segura desde su diseño tecnológico hasta la eficacia jurídica.

III. Evolucionamos con el estado de la arte de las tecnologías de la información y a la vanguardia de las tendencias normativas y de procedimiento.

"No es posible resolver los problemas de hoy con las soluciones de ayer" Roger Van Oech

GUía

1

SEGURIDAD DE LA INFORMACION

Auditoria de sistemas, análisis de vulnerabilidades, hacking ético, herramientas de monitorización, repositorios comunes de información, virtualización, copias de seguridad, ...

2

COMPLIANCE Y PRIVACIDAD

Protección de datos personales, cumplimento normativo, responsabilidad penal de la empresa, reputación digital , ...

3

AUDITORIA Y CERTIFICACIONES

Auditoria de sistemas y procedimientos según ISO y otros esquemas para la obtención de certificaciones ISO 27000, ISO 20000, ISO 19600, ...

4

PERICIALES Y FORENSICS

Análisis forense de incidentes y accidentes tecnológicos. Robo de información, evidencias electrónicas y preservación de pruebas , ...

ESquema general

- CERTIFICABLE 27701
- SECTORES OBLIGADOS DPD

- SISTEMAS IN HOUSE
- HOSTING o CLOUD
- COMUNICACIONES
- IDENTIFICACION
- BACK UP

GDPR
LOPDGDD

SISTEMAS TI
GOBERNANZA

COMPLIANCE

ISO 27001
ENS

- **COMPLIANCE** 19600 CERTIFICABLE

- ENS: ACREDITABLE
- ISO 27001 CERTIFICABLE

SEGURIDAD DE LA INFORMACION

Auditoria de sistemas, hacking ético, análisis de vulnerabilidades, herramientas de monitorización, repositorios comunes de información, virtualización, copias de seguridad, …

ATAQUES DE CIBERSEGURIDAD 2019

PERFIL — PYMES — +70%

PREVISION — PLAN DE RESPUESTAS — -30%

COSTE — COSTE INCIDENTE

Por incidente 30.700 €
En España 1,140 mill €

INCREMENTO — ATAQUES de 2017 a 2018 — +40%

"Sacrificar la innovación para ahorrar costes, es como parar el reloj para ahorrar tiempo"

INCIDENTES 2018-2021

38.192 brechas de seguridad en España en 2018

60% de los incidentes son desde el interior

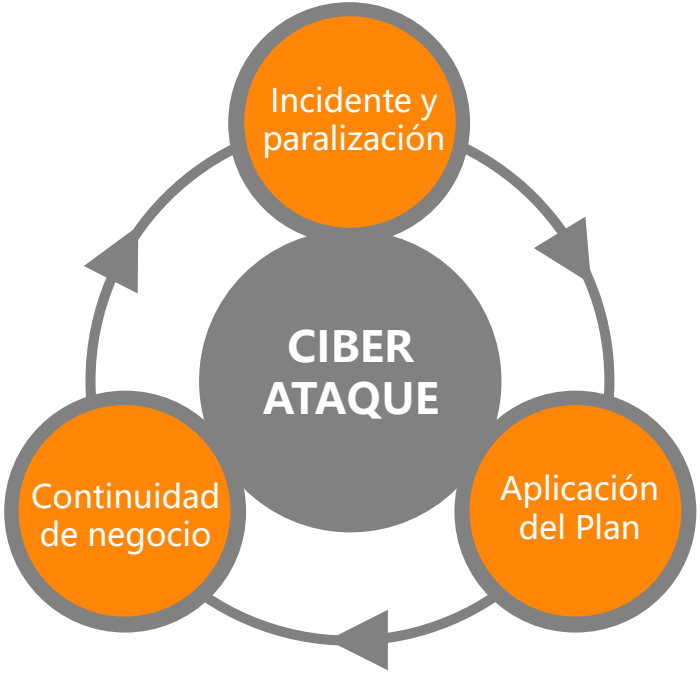
6.000 millones de perdidas por ciberseguridad en 2021

1.000 millones de gasto en ciberseguridad en los últimos 5 años

Costes por ransomware han aumentado **57 veces** desde 2015

ccn-cert

ACTUACION



INCIDENTE Y PARALIZACION

Detectado el ataque, paralización de procesos y contención del incidente.

APLICACION DEL PLAN

Procedimientos y manual de actuación. Comité de crisis y aplicación de medidas.

CONTINUIDAD DE NEGOCIO

Centro de control. Equipos de redundancia. Servidores espejo. Copia de seguridad.

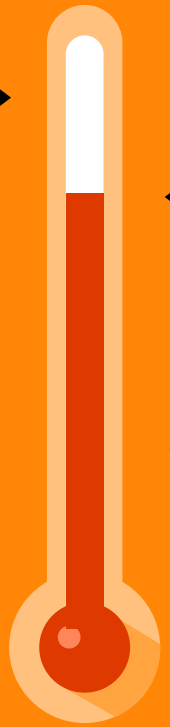
ANALISIS DE ACTUACION

Conservación de trazas, "logs" y evidencias electrónicas. Análisis de daños y tiempos de actuación. Evaluación de actuaciones. Análisis del ataque. Investigación forense. Informe de mejoras.

MATRIZ DE RIESGO

INCERTIDUMBRE

Para aquellos riesgos que no se pueden prever , la solución esté en el aseguramiento



PROBABILIDAD

Nivel o porcentaje de que ocurra, de nula, poco probable, muy probable, casi seguro

EFECTOS

Operativos, económicos o de responsabilidad. bajos, medios altos o muy altos

100%

- **PORCENTAJE DE PREVISION**

Ajustando la matriz de riesgo con los efectos personales y económicos, la probabilidad de que ocurra, y complementando lo improbable con el aseguramiento y el riesgo se aproxima a 0%

HERRAMIENTAS ESENCIALES

PLANIFICACION

Análisis de riesgos
Securizacion
Monitorizacion
Plan de contingencia
Plan de actuación
SOC

RESPALDO

Servidores espejo
DNS alternativos
Copias de seguridad
Datos y estructura
Centro de control alternativo y descentralizado

RECUPERACION

Plan de actuación
Bloqueo del atacante
Redireccionamiento
Recuperacion de control
Restauración de estructura y datos

PORCENTAJE DE EXITO

VARIABLES

Tiempo de detección y reacción

Profundidad y gravedad del ataque

Tiempo de recuperación

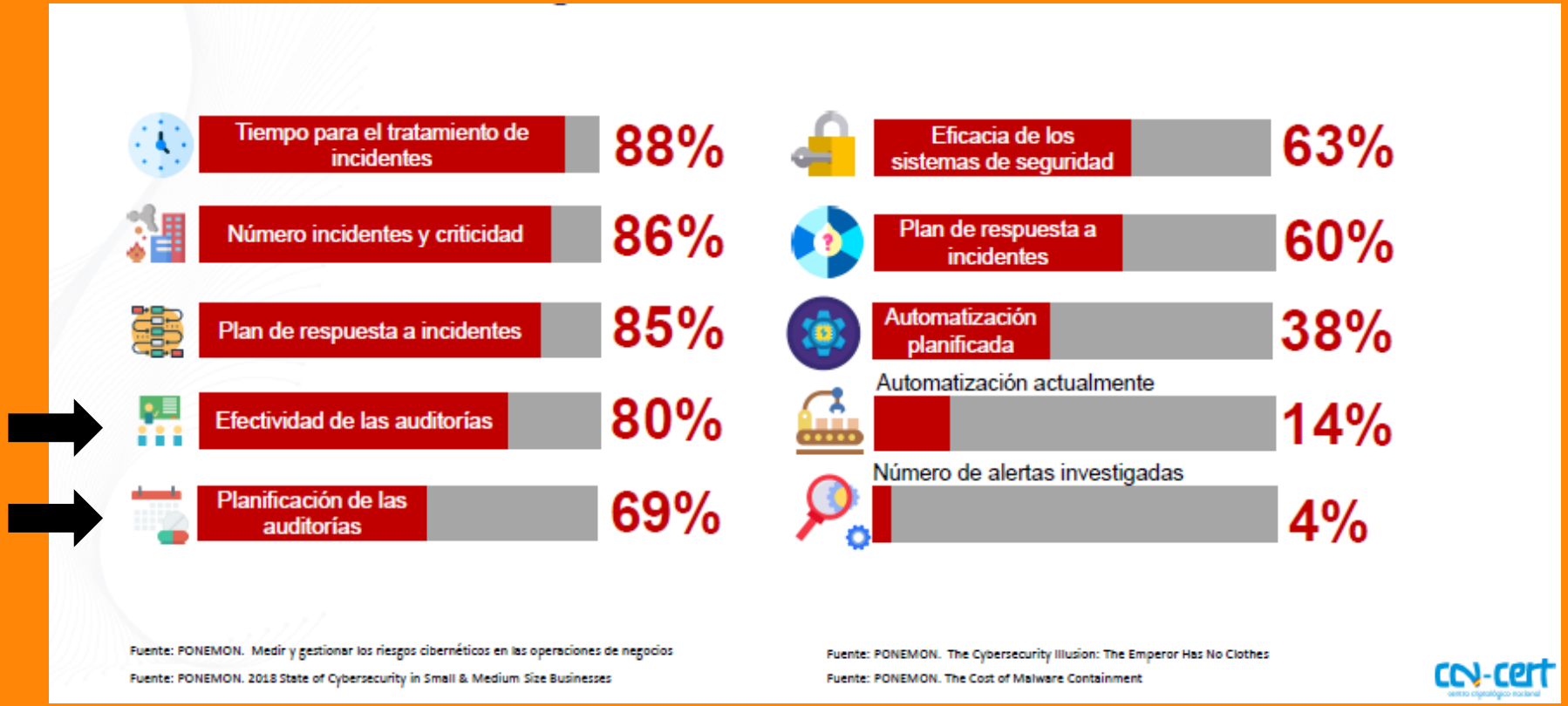
Previsión de daños e informe forense

Análisis de vulnerabilidades e informe de mejoras

COMPLIANCE Y PRIVACIDAD

Protección de datos personales, cumplimento normativo, responsabilidad penal de la empresa, reputación digital , ...

METRICAS DE CIBERSEGURIDAD



INCIDENTES DE SEGURIDAD

30%

INCIDENTES EXTERNOS

Ataques aleatorios externos. Incidentes por corte de energía o corte de líneas de comunicación. Averías de servidores y equipos. Accidentes y siniestros físicos.

70%

INCIDENTES INTERNOS

Competencia desleal y espionaje industrial. Gestion de despidos y expedientes de regulación de empleo. Administración negligente o desleal. Robo de información y chantaje. Fraude fiscal y blanqueo de capitales.

RIESGOS

ESTATUS

Auditoria con esquemas antiguos
Plan de Seguridad anticuado
Ausencia Plan Contingencia
Sistemas de información obsoletos
Falta de Formación
Complacencia

VARIABLES

Nueva Legislación
Nuevas obligaciones
Nuevos Retos
Nuevas Aplicaciones
Nuevas Amenazas.

DESEQUILIBRIO DE PLAN DE RIESGOS

SERVICIOS

1

HACKING ETICO

Reconocimiento activo y pasivo
Análisis de vulnerabilidades
Accesos y permanencia
Informe de actuación
Propuestas de soluciones

2

COMPLIANCE PENAL

Identificación y diagnóstico
Matriz de riesgos
Planificación
Implantación y concienciación
Evaluación y ajuste

3

ISO 27701 PRIVACIDAD

Evaluación de impacto
Auditoria y comprobación
Corrección de deficiencias
Designación DPO

4

PERDIDA DE INFORMACION

Detección de pérdida o copia de información sensible
Tasación del posible daño
Proceso forense e investigación

5

ISO 27000 y ENS SEGURIDAD INFORMACION

Sistemas de gestión de información
Copias de back-up
Cifrado de información
Eliminación de procedimientos con riesgo

OPORTUNIDAD Y MEJORA

La privacidad es una oportunidad para mejorar los sistemas

FASES IMPLANTACION GDPR

DPIA

Plan de evaluacion de impacto. Matriz de reisgos. Obligaciones procedimentales y legales

AUDIT

Detección de errores y deficiencias. Informe de situación. Propuesta de actuaciones. Errores de procedimiento. Riesgos reputacionales

PLAN

Plan de actuación y corrección. Política de accesos y de gestión de información. Plan de contingencia y actuación ante perdida o fuga de información

DPO

Control permanente sobre la gestión de datos personales. Coordinación de actuaciones. Centralizador en caso de incidente, Interlocución ante la Autoridad Nacional.

ACTUACIONES

PLANIFICACION

Desarrollo de actuaciones ajustadas a la necesidad real de la empresa y de su información

COMPROMISO

De la Direccion y de la Consultora para obtener el óptimo resultado

DPO-DPD

Mantenimiento de la vigilancia y control de procesos. Respaldo frente a errores e inspecciones

IMPORTANTE

REGLAMENTO (EU) Y LEY (LO) DE PRIVACIDAD

El Reglamento Europeo UE 679/2016 ha supuesto un cambio de paradigma en el tratamiento de datos personales que afecta a la muchos de los procedimientos de la empresa
Y la Ley Orgánica 3/2018 supone la obligatoriedad sin demora de medios y recursos para el cumplimiento de la norma que afecta tanto a Mapa de Riesgos, como Plan de Impacto y la designación de un Delegado de Protección de Datos capacitado, en ciertos casos obligatorio, y en la mayoría recomendable. La Auditoria se transforma en Proceso

AUDITORIA Y CERTIFICACIONES

Auditoria de sistemas y procedimientos según ISO y otros esquemas para la obtención de certificaciones ISO 27000, ISO 20000, ISO 19600, …

INTERRELACION

COMPLIANCE

El complimiento normativo exige un esfuerzo de la organización en desarrollar y testar sus procedimientos

SEGURIDAD

Una seguridad planificada demanda una matriz de riesgos, un plan de impacto y un plan de contingencia.

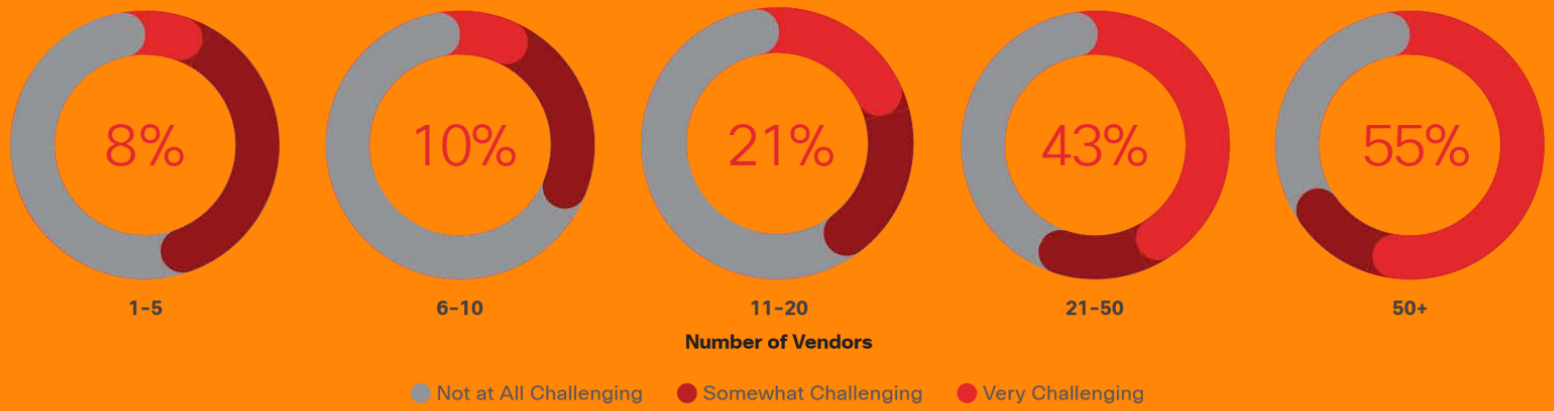
La continuidad de negocio depende de su permanente revisión La SEGUIRDAD es un PROCESO, no un producto ni un servicio.

EL NUMERO DE PROVEEDORES INCREMENTA EL RIESGO

As vendors increase, so does the challenge of orchestrating security alerts

Source: Cisco 2018 Security Capabilities Benchmark Study

Challenge of Orchestrating Multiple Vendor Alerts
IT Security Personnel with:



	Education	Financial Services	Government	Healthcare	Manufacturing	Pharma	Retail	Telecom	Transportation	Utility/ Energy
Very Challenging	17%	24%	16%	42%	14%	25%	19%	14%	12%	27%

CERTIFICACIONES y NORMAS

1

SEGURIDAD DE LA INFORMACION

ISO 27000 y ss, 20000 y ss: Seguridad de la information
ENS Esquema Nacional de Seguridad y CCN CERT

2

COMPLIANCE y PERICIALES

ISO 19600 Compliance
ISO 19700 Evidencias digitales y periciales

3

CLOUD COMPUTING y GESTION DOCUMENTAL

ISO 27032 Cloud Computing, CSA y StarAudit
ISO 15489, 19005, 18492, 23081, 26122 … y Moreq, Gestion Documental

4

SEGURIDAD

22301 Continuidad de Negocio y ANSI/ASIS
UNE 50518 Centrales de Alarma

MARCOS DE REFERENCIA Y BUENAS PRACTICAS

- ENS + guías STIC
- ISO 27000
- NIST 800-53
- LPIC (en caso de infraestructuras críticas)

Fuente: CCN-Cert

Fuente: AENOR

ccn-cert
centro criptológico nacional

ESQUEMAS DE CERTIFICACION

VENTAJAS DE LA AUDITORIA Y CERTIFICACION

El uso de las normas ofrece herramientas empresariales y de marketing potentes a organizaciones de cualquier tamaño.

Se pueden utilizar para ajustar de los objetivos de la empresa y gestionar los riesgos

Se trabaja de un modo más eficaz y con modos y procesos más sostenibles.

Permitirán demostrar la calidad de su producto servicio a los clientes y proveedores y sirve como elemento de control a las AAPP y a la subcontratación

Ayudan a integrar las mejores prácticas en la organización, y fomenta la continua mejora.

Incrementan las posibilidades de innovación y excelencia en la empresa.

PERICIALES Y FORENSICS

Análisis forense de incidentes y accidentes tecnológicos. Robo de información, evidencias electrónicas y preservación de pruebas , ...

CAUSALIDAD INCIDENTE

SEGURIDAD INTERNA

Procedimientos
inexistentes o
no aplicados
Falta concienciación

MEDIOS TECNICOS

Medios obsoletos
proveedor NO confiable
software NO original
Falta conocimiento

CIBER DELINCUENTE

interno/externo
Ataque como fin
Ataque como medio
Sabotaje

INCIDENTE

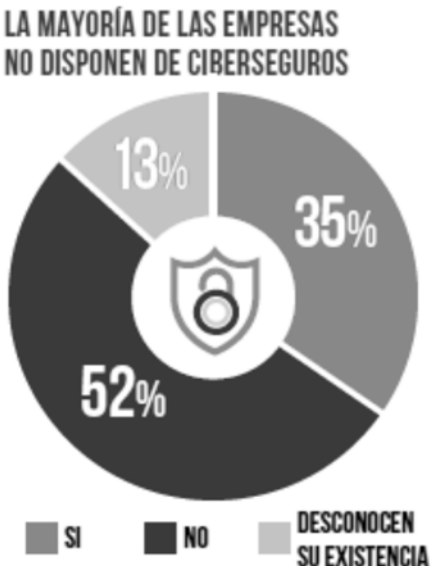
Perdida económica
Perdida patrimonial
Perdida reputacional
Indemnización/sanción

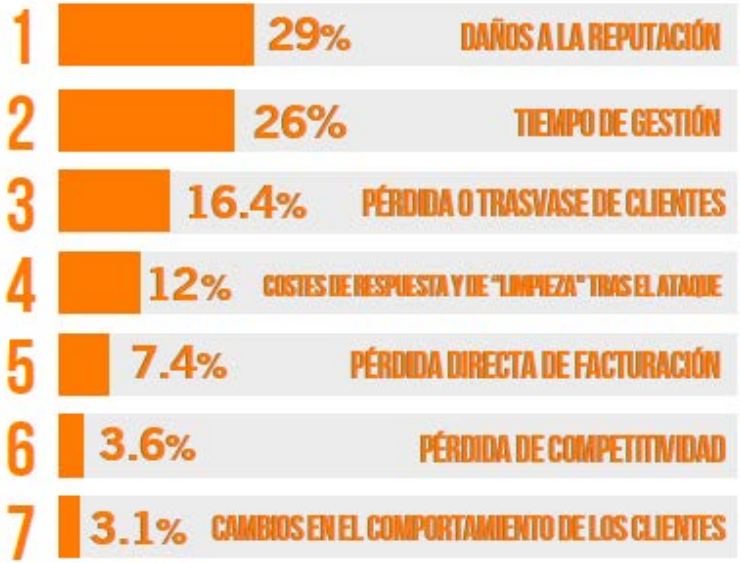
Las probabilidades de un incidente crecen exponencialmente por la suma de riesgos no valorados adecuadamente

CONSECUENCIAS CIBERATAQUES

"EL CHANTAJE Y LA EXTORSIÓN SE CONSIDERAN TRADICIONALMENTE COMO VARIANTES BURDAS DEL CRIMEN FINANCIERO. PERO EN EL MUNDO DIGITAL SON ACTIVIDADES SORPRENDENTEMENTE ORGANIZADAS"

PAUL JACOBS, LÍDER GLOBAL DE CIBERSEGURIDAD





Datos Estadisticos

International Business Report Grant Thorton

PRECAUCIONES BASICAS

CONEXION

Conexión de seguridad https://
Verificar certificado del proveedor

CHEQUEO

Sistema operativo actualizado
Programas con licencia
Correos y aplicaciones de pago
Antivirus operativo
Firewall activado

PROVEEDOR

Aviso legal, Privacidad y Condiciones del proveedor de servicios muy definidos
Seguridad del medio de pago
Domicilio y contacto para el caso de conflicto o reclamación

RECOMENDACIONES

https://www.osi.es/es

INSTITUCIONES PUBLICAS

- La Estrategia de Ciberseguridad Nacional sirve de fundamento al Gobierno de España para desarrollar las previsiones en materia de protección del ciberespacio con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas.

- El grado de dependencia de nuestra sociedad respecto de las TIC y el ciberespacio crece día a día. Conocer sus amenazas, gestionar los riesgos y articular una adecuada capacidad de prevención, defensa, detección, análisis, investigación, recuperación y respuesta constituyen elementos esenciales de la política de seguridad.

CCN-cert centro criptológico nacional

ens Esquema Nacional de Seguridad

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

aepd agencia española protección datos

GRUPO DE DELITOS TELEMÁTICOS

BIT

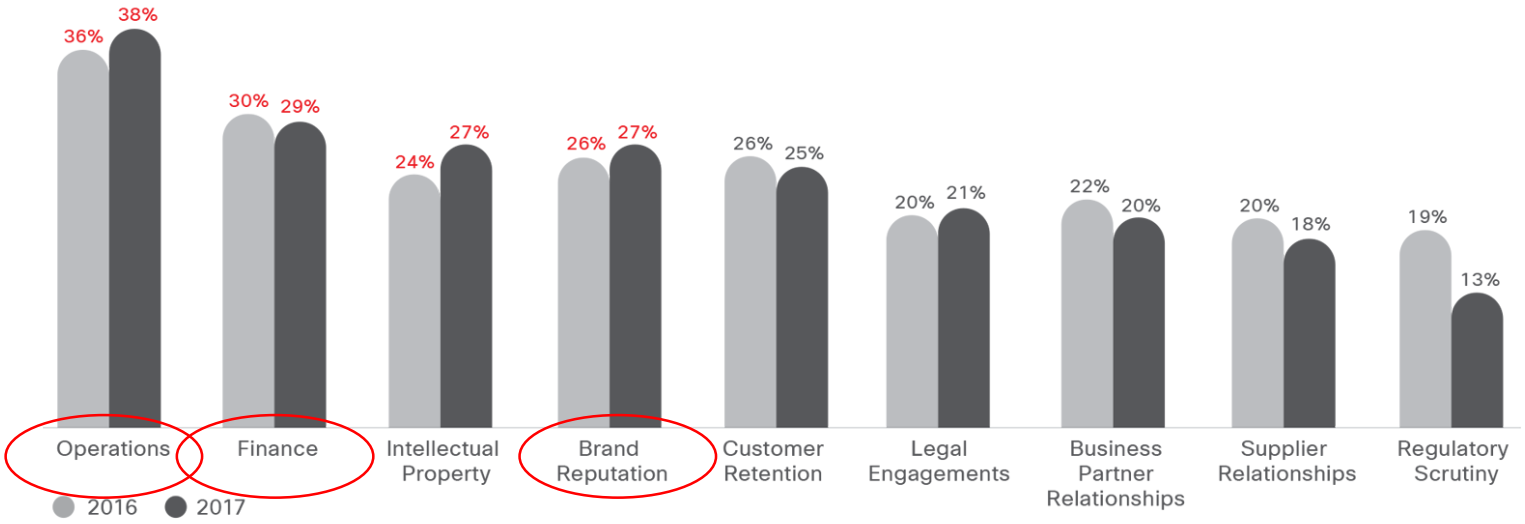
CNPIC CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

eni Esquema Nacional de Interoperabilidad

AMBITOS AFECTADOS

Operations and finances most likely to be affected by security breaches

Source: Cisco 2018 Security Capabilities Benchmark Study



For more info visit: **cisco.com/go/acr2018**

cisco

RECURSOS

LAS PERSONAS

En cualquier empresa, *los recursos humanos* son los que determinan los objetivos y los medios para obtener sus fines, los que llevan a cabo los avances, los logros y los errores de las organizaciones. Constituyen su recurso más preciado, y valioso

添加相关文字内容

添加相关文字内容

CONFIANZA y EQUIPO

"La confianza viene de horas, días, semanas y años de constante trabajo y dedicación" **Roger Staubach.**

LAS PERSONAS

AE Abogados y Economistas expertos en Tecnologías de la Información, Cumplimiento Normativo y Privacidad.

IT Ingenieros de Telecomunicaciones e Informática especializados en Ciberseguridad, redes, SAP, ….

DP Auditores certificados DPO (Delegado Protección de Datos) Directores de Seguridad y expertos en Seguridad Privada

PF Peritos Forenses y Tasadores Judiciales de sistemas TIC, evidencias electrónicas, videovigilancia y sistemas de seguridad.

CA Consultores y Auditores certificados normas UNE/ISO, (seguridad calidad y compliance) Star Audit, e ISACA

ASOCIACIONES

APEP PRIVACIDAD

ASIS ESPAÑA

AECRA SEGURIDAD

EUROCLOUD

PETEC PERITOS TIC

ISACA AUDITORIA

REFERENCIAS

GESYS ABOGADOS

BBVA

GRUPO TUDIC CONSTRUCCIONES
REHABILITACIONES Y CONSTRUCCIONES TUDIC S.L.

Techco security

FIPSE FUNDACIÓN PARA LA INNOVACIÓN Y LA PROSPECTIVA EN SALUD EN ESPAÑA

ce consulting empresarial

Santander

ACEK

MIRNAX

DERMA INNOVATE

coteco

ProA CAPITAL

StreamGPS

FAECP Fundación Asociación Española de Coloproctología

F.Tomé Volkswagen

evicertia EVIDENCIAS CERTIFICADAS

Monarque Hotels

SETS

tyco Integrated Fire & Security

SOCIEDAD ESPAÑOLA DE NEUROCIENCIA

geq GARCIA-ECHAVE ABOGADOS

isquaemia BIOTECH

CLÍNICA DERMATOLÓGICA INTERNACIONAL

Drams TECNOLOGÍA – SEGURIDAD

Bodybell PERFUMERIAS

eqm Fundada en 1986

seco sociedad española de cirugía de la obesidad

SEDAR Sociedad Española de Anestesiología, Reanimación y Terapéutica del Dolor

cepyme CONFEDERACIÓN ESPAÑOLA DE LA PEQUEÑA Y MEDIANA EMPRESA

RENOIR

CEOE CONFEDERACIÓN ESPAÑOLA DE ORGANIZACIONES EMPRESARIALES

VALVONTA

Auditoria y Seguridad

www.valvonta.es